Datenschutzgerechtes eGovernment

An der Ausarbeitung der Handreichung „Datenschutzgerechtes eGovernment“, für die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2001 eine Arbeitsgruppe eingesetzt hat, waren Mitarbeiter der Landesbeauftragten für den Datenschutz Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Thüringen und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein sowie des Bundesbeauftragten für den Datenschutz und des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) beteiligt. Begleitet wurden die Arbeiten von den Professoren Dr. Alexander Roßnagel (Universität Kassel) und Dr. Klaus Lenk (Universität Oldenburg) sowie seitens der Begleitforschung zu Media@Komm durch Herrn Dr. Eifert (Hans-Bredow-Institut Hamburg). Die Leitung der Arbeitsgruppe lag bei dem Landesbeauftragten für den Datenschutz Niedersachsen.

Der Text der Handreichung ist auch im Internet unter der Adresse www.lfd.niedersachsen.de oder www.datenschutz.de verfügbar. Redaktionsschluss war der 30. November 2002. Die Arbeitsgruppe wird unter Berücksichtigung aktueller Entwicklungen diese Handreichung fortschreiben. Hinweise und Beschreibungen weiterer Referenzanwendungen sind erwünscht. Ansprechpartner ist Herr Thomas Knaak (thomas.knaak@lfd.niedersachsen.de).

Herausgeber: Der Landesbeauftragte für den Datenschutz Niedersachsen
Brühlstr. 9, 30169 Hannover
Postfach 2 21, 30002 Hannover
Tel.: 0511/120-45 00
Fax: 0511/120-45 99
eMail-Adresse: poststelle@lfd.niedersachsen.de
Verantwortlich Burckhard Nedden

Umschlagslayout: grafolux
Kambriumweg 9, 30455 Hannover

Gesamtherstellung: Schlütersche Druck GmbH&Co.KG
Hans-Böckler-Straße 52, 30851 Langenhagen

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende grammatische Geschlecht verwendet. Selbstverständlich richtet sich dieser Text an die Angehörigen beider Geschlechter.

Inhaltsverzeichnis

1 eGovernment und Datenschutz: Wie passt das zusammen?

1.1 Verwaltung im Umbruch

Mit dem Begriff „Verwaltung“ assoziieren die meisten verstaubte Akten, riesige Registraturen und Altablagen mit unzähligen papiernen Dokumenten. So hat die Verwaltung jahrhundertelang gearbeitet und hat aus dieser Arbeitsform auch ihre Legitimation abgeleitet. Wer kennt nicht den Satz „quod non est in actis, non est in mundo“ oder die besondere Betonung der Schriftlichkeit als eines wichtigen Wertekriteriums beim Bürokratiemodell Max Webers. Heute arbeitet die Verwaltung zunehmend mit Informationen, die elektronisch gespeichert und übertragen werden. Diese Informationen sind ohne technische Hilfsmittel nicht einsehbar und lesbar, ihre inhaltliche Richtigkeit ist ohne Technik nicht prüfbar und es ist nicht nachvollziehbar, in welcher Weise, zu welchem Zweck und von wem die Informationen weiterverarbeitet worden sind. Wenn solche Informationen, wie dies bei den allermeisten einzelfallbezogenen Informationen in der Verwaltung der Fall ist, einen Bezug zu einer bestimmten oder bestimmbaren Person haben, ist der Betroffene bei elektronisch gespeicherten Informationen daher von vornherein schlechter gestellt als bei analoger Verarbeitung, wo er ohne technische Hilfsmittel Einsicht nehmen und Verarbeitungsschritte nachvollziehen kann.

Gleichzeitig verändert sich die Struktur der Datenhaltung in der modernen Verwaltung. Nicht mehr einzelfallbezogen angelegte Aktenstücke, die als „Originale“ in den bearbeitenden Organisationseinheiten weitergereicht werden, bestimmen das künftige Bild, sondern zentrale oder verteilte Datenbestände in elektronischen Datenspeichern mit Zugriffsmöglichkeiten unterschiedlicher Stellen. Die Einhaltung von Zweckbindung und informationeller Gewaltenteilung ist nicht mehr ohne weiteres „offensichtlich“ und damit nachvollziehbar zu machen. Es wächst die Gefahr, dass Informationen, die über den Einzelnen in der Verwaltung vorhanden sind, auf den berühmten Knopfdruck hin blitzschnell zusammengeführt werden. Profilbildungen sind möglich, die in der analogen Welt der Papierakten schon wegen des großen Aufwandes nur ein äußerst geringes Gefährdungspotential darstellen.

Beim eGovernment werden die Möglichkeiten der elektronischen Information und Kommunikation sowie vor allem auch der elektronischen Transaktion über das Internet zielbewusst und konsequent eingesetzt, um – ganz im Interesse der Bürgerinnen und Bürger – Verwaltungsvorgänge und Entscheidungsabläufe zu beschleunigen, um besser und schneller und mit einer Orientierung als Dienstleister auf Anträge und Anliegen reagieren zu können, um für die Bürgerinnen und Bürger neue Möglichkeiten des Zugriffs auf Informationen der Verwaltung oder der demokratischen Teilhabe zu entwickeln. Aber es bedeutet andererseits auch, dass die Gefahrenpotentiale für die informationelle Selbstbestimmung der Betroffenen größer werden. Die Verarbeitung von personenbezogenen Informationen erfolgt beim eGovernment nicht mehr nur in einer eindeutig lokalisierbaren und einem bestimmten Verantwortlichen fest zuordnenbaren Datenverarbeitungsanlage, sondern in behördenübergreifenden Netzen oder sogar im weltweiten Verbund des Internet mit einer unübersehbaren Zahl von Beteiligten und Nutzern. Wie kann hier noch sichergestellt werden, dass – wie das Bundesverfassungsgericht es im Volkszählungsurteil als Grundlage des informationellen Selbstbestimmungsrechts gefordert hat – jeder selbst bestimmen

nellen Selbstbestimmungsrechts gefordert hat – jeder selbst bestimmen kann, wer was wann bei welcher Gelegenheit über ihn weiß?

1.2 Ziele und Aufbau der Handreichung

eGovernment wird die Verwaltung schneller, einfacher, effektiver und transparenter machen und damit die Erwartungen, die die Menschen an eine moderne Verwaltung haben, noch besser erfüllen können. Diese Handreichung will dazu beitragen, dass bei der Entwicklung von eGovernment-Lösungen die Anforderungen von Datenschutz und Datensicherheit im Blick bleiben, und praktische Hinweise dafür geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können. Nur dann, wenn eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz der personenbezogenen Daten gewährleistet ist, wird auch die notwendige Akzeptanz für eGovernment-Anwendungen auf Seiten der Bürgerinnen und Bürger sowie der anderen „Kunden“ der Verwaltung zu erreichen sein.

Die Handreichung gliedert sich wie folgt:

- Im **Kapitel 2** werden einleitend **Erscheinungsformen und Modelle** des eGovernment beschrieben und die bisherigen Ansätze und die voraussichtliche weitere Entwicklung beim eGoverment zusammenfassend bewertet.
- Das **Kapitel 3** stellt die **allgemeinen Anforderungen** an eGovernment aus Sicht von Datenschutz und Datensicherheit dar, wie sie sich aus den rechtlichen Rahmenbedingungen sowie den technischen und organisatorischen Sicherungszielen ergeben, ohne grundsätzlich schon auf Umsetzungsmöglichkeiten oder auf einzelne Anwendungen einzugehen. Außerdem werden das Zusammenspiel der gesetzlichen Grundlagen, die Datenverarbeitung durch Dritte, die elektronische Signatur, der Stellenwert des Zugangs zu öffentlichen Informationen beim eGovernment sowie die Notwendigkeit von Standardisierungen behandelt.
- Das **Kapitel 4** stellt in komprimierter Form die allgemeinen und spezifischen **Bedrohungen** dar, die sich bei eGovernment-Anwendungen für Datenschutz und Datensicherheit ergeben. Dies kennzeichnet gleichzeitig die Herausforderungen, die zu bewältigen sind.
- Im **Kapitel 5** werden für die Umsetzung der datenschutzrechtlichen Anforderungen beim eGovernment **konkrete umsetzungsorientierte Handlungsempfehlungen** gegeben; es schließt insoweit an die Darstellung in Kapitel 3 an. Hier finden sich zahlreiche Praxishinweise, wie eine sichere und vertrauliche Kommunikation, wie angemessener Datenschutz und die erforderliche Datensicherheit bei den verschiedenen eGovernment-Anwendungen zu erreichen sind. Mit dem Begriff „Handlungsempfehlungen“ soll zum Ausdruck gebracht werden, dass dazu aktives Tun und gezieltes Vorgehen gefragt sind, denn die genannten Ziele stellen sich nicht von selbst ein, sondern erfordern die Vorkehrungen, die in diesem Kapitel dargestellt sind.
- Im **Kapitel 6** sind technische und organisatorische Werkzeuge zur Bewältigung der in Kapitel 4 dargestellten Herausforderungen in Form eines **Baukastens** zusammengestellt. Zusammen mit den Handlungsempfehlungen in Kapitel 5 ergeben sie eine Art **„Check-Liste“,** anhand derer überprüft werden kann, welche Maßnahmen und Vorkehrungen zur Gewährleistung einer datenschutzgerechten

und sicheren eGovernment-Anwendung getroffen werden müssen. Im Abschnitt 6.3 sind die für eine datenschutzfreundliche Lösung wichtigsten Selbstschutzmaßnahmen zusammengestellt.

- ☞ Im **Kapitel 7** sind **Referenzanwendungen** für Praxislösungen des eGovernment aufgeführt. Damit soll nicht nur ein Beitrag zur Herausbildung von möglichen Muster- und Standardanwendungen geleistet, sondern zugleich auch der Beleg dafür geliefert werden, dass datenschutzfreundliche Lösungen beim eGovernment möglich und wirtschaftlich zumutbar sind. Die Referenzlösungen sind von der zuständigen Datenschutzaufsicht datenschutzrechtlich bewertet worden und können daher grundsätzlich als Lösungsansatz empfohlen werden.

Wir möchten mit dieser Handreichung alle diejenigen erreichen, die in den Verwaltungen an zentraler Stelle als Verwaltungschefs, als Organisatoren, als Verfahrensentwickler, als IT-Verantwortliche, als interne Datenschutzbeauftragte oder als Personalvertretungen den Weg ins eGovernment vorbereiten oder schon umsetzen. Wir wenden uns aber natürlich auch an alle, die in den Verwaltungen mit eGovernment-Anwendungen aktuell oder künftig arbeiten, und an die Bürgerinnen und Bürger, an die Wirtschaftunternehmen und an die anderen „Kunden“ der Verwaltung, die die neuen Angebote im eGovernment nutzen. Für die Nutzerinnen und Nutzer sind die Hinweise und Empfehlungen besonders wichtig, die sich auf Instrumente zum Selbstdatenschutz beziehen (vgl. dazu insbesondere Kapitel 6.3). Denn ein Teil der Verantwortung für den Schutz und die Vertraulichkeit ihrer Daten verbleibt auch weiterhin bei den Betroffenen selbst und kann auch nur von ihnen durch Nutzung der in der Handreichung genannten Selbstschutzinstrumente ausgefüllt werden.

2 Erscheinungsformen und Modelle

2.1 Definition und Ziele von eGovernment

Der Begriff eGovernment – zusammengesetzt aus den beiden Wörtern „electronic “ (engl.: elektronisch, rechnergestützt) und „Government “ (engl.: Verwaltung, Regierung) – bezeichnet die Bemühungen der öffentlichen Verwaltung, ihre Aufgaben und die darauf bezogenen Verwaltungsabläufe mittels der modernen Informations- und Kommunikationstechnologie zu erfüllen. Dabei steht die Nutzung des World Wide Web, also des Internets, häufig als Medium im Mittelpunkt der Betrachtung. eGovernment ist gleichsam Synonym für die Modernisierung der überkommenen aktendominierten Verwaltung im Back- und Front-Office-Bereich, für Aufbruchstimmung und den IT-Einzug in die Verwaltungsstrukturen auf unterschiedlichen Ebenen. Entsprechend muss dem Begriff, orientiert an den speziellen Verwaltungsanforderungen und -aufgaben der Behörde, auch ein eigener Bedeutungsinhalt gegeben werden. Auszugehen ist von folgender Grunddefinition:

eGovernment bezeichnet die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung sowie der Leistungserstellung und –abwicklung in Politik, Regierung und Verwaltung unter Nutzung der modernen Informations- und Kommunikationstechniken, insbesondere des Internet. Einbezogen ist der gesamte öffentliche Sektor.

Drei Interaktionsformen sind bestimmend für Aufbau, Struktur und Abwicklung von eGovernment, nämlich Information, Kommunikation und Transaktion.
Diesen drei Formen können nahezu alle Aktivitäten im Bereich des eGovernment zugeordnet werden. Nach einem vorsichtigen Anfang im Bereich der Information (z. B. Öffnungszeiten des Hallenbades) ist zurzeit der Schwerpunkt der Aktivitäten noch im Bereich der Kommunikation (z.B. eMail-Kontakt zur Verwaltung) angesiedelt. Als Kernbereich von eGovernment muss jedoch die Transaktion gesehen werden, also die für beide Seiten verbindliche und möglichst vollständige Abwicklung von Verwaltungsaufgaben unter Einschluss der abschließenden Entscheidung und deren Bekanntgabe auf elektronischem Wege.

2.2 Binnenorientierte Veränderungen

Verwaltungsmodernisierung über eGovernment hat einen externen und einen internen Anknüpfungspunkt. Schwerpunkt der Betrachtung der Bürgerinnen und Bürger ist im Regelfall die Frage, wie die Behörde mit ihnen (extern) kommuniziert. Daneben müssen aber auch die behördeninternen Veränderungen gesehen werden. Die über Jahrzehnte gewachsenen Aufbau- und Ablaufstrukturen der Behörden müssen überdacht, Verwaltungsverfahren analysiert und auf ein Zusammenwirken mit vor- und nachgelagerten Prozessen überprüft werden. Eingefahrene Strukturen sind zu entflechten, zu vereinfachen und Standardisierungen zu entwickeln, gesetzliche und verordnungsrechtliche Zuständigkeiten sind zu überarbeiten. In diesem internen Bereich wird der größere und von der Öffentlichkeit weniger beachtete Arbeitsaufwand für die Behörden liegen. Entscheidend ist, dass dieser Aufwand im Vorfeld betrieben wird, bevor sich die Verwaltung online auf die Bürgerinnen und Bürger zubewegt. Erst die konsequente Umsetzung dieser grundlegenden internen Organisationsentwicklungsmaßnahmen über die Verwaltungsgrenzen hinaus ermöglicht den gewünschten Erfolg der darauf aufbauenden Online-Verwaltung.

2.3 Erscheinungsformen und Beziehungsgeflechte

Die nach außen sichtbare Darstellung von eGovernment findet sich vermittelt über die elektronischen Medien im Internetauftritt der jeweiligen Behörde. Hier sind unterschiedliche Inhalte und Intentionen in einem häufig bunten Strauß von Websites zusammengebunden. eGovernment im kommunalen Bereich deckt in der Regel schwerpunktmäßig folgende drei Bereiche ab: das Leben in der Region, den Marktplatz und die elektronischen Verwaltungsdienste. Diese drei Komponenten finden sich fast in jedem Internetportal einer Kommune wieder und werden von unterschiedlichen Interessenträgern mit Leben gefüllt.

Zentrale Säule dieser Struktur für das eGovernment und Ausdruck der Erfüllung gemeindlicher Aufgaben als Angelegenheiten der örtlichen Gemeinschaft und im Bereich des übertragenen Wirkungskreises sind die elektronischen Verwaltungsdienste. Hier werden Informationen eingestellt, Kontaktadressen, Telefonnummern und eMail-Adressen angegeben, Formulare zum Download oder auch zum Ausfüllen direkt am Bildschirm und zum Zurücksenden online angeboten, getreu dem Motto: „Die Daten und nicht die Bürger sollen laufen!“ Mittelfristig werden über diese Säule auch Verwal-

tungsakte erlassen und der Bürgerin und dem Bürger bekannt gegeben werden können.
Vergleichbares gilt für die Verwaltungsebenen der Länder und des Bundes.

eGovernment ist nicht allein im Verhältnis zwischen Verwaltung und Bürgerschaft anzusiedeln. Außer ihnen wirken weitere Akteure mit, nämlich die Politik, die Wirtschaft sowie Organisationen und Verbände, die mit ihnen und untereinander vielfältig verflochten sind.

Im Verhältnis der Verwaltung zu den Bürgerinnen und Bürgern schiebt sich unter dem Gesichtspunkt der Dienstleistung auf kommunaler Ebene zunehmend das „Lebenslagenprinzip“ in den Vordergrund. Im Fall des Umzugs oder der Heirat o.Ä. muss die Bürgerin oder der Bürger nicht mehr von Amt zu Amt laufen. Der Service liegt in der Bündelung bei einer Anlaufstelle.

Bei den Verbindungen zwischen der Behörde und der Wirtschaft geht es auch um Standortförderung und –pflege im weitesten Sinne. Dazu gehören neben umfänglicher Information über Ansprechpartner, Planungsgrundlagen und Leistungsangebote die Verfahrenstransparenz und die zügige Erteilung von beantragten Genehmigungen, die demnächst vollständig online und - soweit möglich - ohne Medienbrüche erteilt werden sollen.
Auch die Politik wird eGovernment nutzen. Der politische Willensbildungsprozess der Parteien, von Fraktionen und Mandatsträgern wird mit Hilfe von eGovernment die Einbeziehung von Bürgerinnen und Bürgern verstärken können und dadurch neue Impulse für partizipative Prozesse und Bürgerengagement geben.

Auch die sonstigen am Gesellschaftsprozess beteiligten Akteure, wie Gewerkschaften, Arbeitgeberverbände, Kirchen, Berufsverbände, Interessenvereinigungen aus allen Lebensbereichen finden im eGovernment ein Forum zum Transport von Informationen und zur Kommunikation und können dies zur Intensivierung ihrer Mitwirkungsfunktionen nutzen.

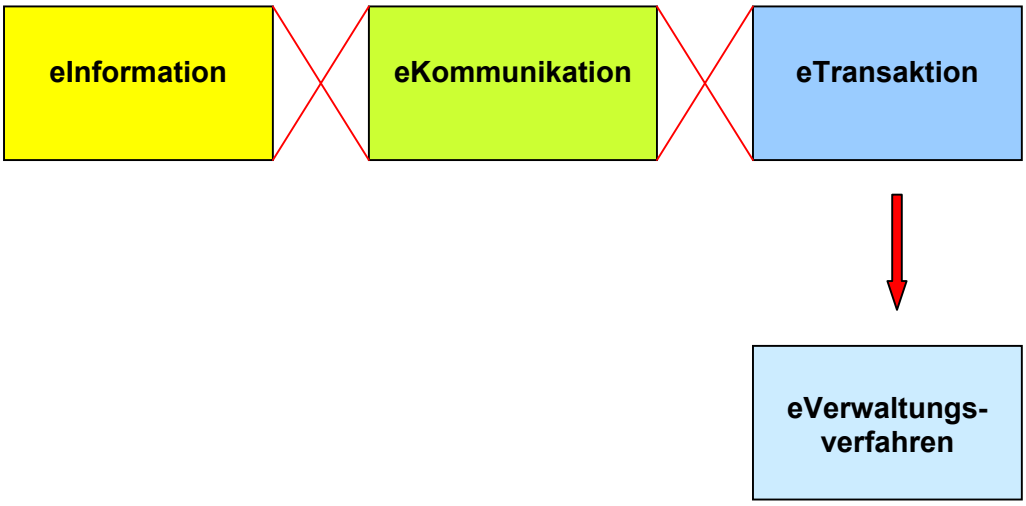
Neue Kooperationsformen schaffen intensive Verknüpfungen zwischen einer Vielzahl von Behörden, Verwaltungsträgern und sonstigen Einrichtungen im öffentlichen Sektor (Kooperierende Verwaltung). Völlig neuartige Kooperationen über Entfernungen und Organisationsgrenzen hinweg werden unter anderem die Ansiedlung und Auslastung von Spezialisten von den Beschränkungen lösen, die sich heute aus der Größe der Verwaltungsbehörden und ihrer Einzugsgebiete ergeben. Verwaltungen werden sich darüber hinaus mit Unternehmen in Netzwerken organisieren. Diese Form der Kooperation (Public-Private-Partnerships) eröffnet neue Möglichkeiten der Aufspaltung von Prozessen auf unterschiedliche Bearbeitungsinstanzen.

2.4 Modelle für eGovernment

Die Vielfalt der oben skizzierten Erscheinungsformen und Beziehungsgeflechte des eGovernment in eindeutig definierte „Modelle“ elektronischer Verwaltung zu übertragen, wird sich bei einem so jungen und dynamischen Themenkomplex wohl kaum allgemein verbindlich erreichen lassen. Denn schon die an der Realisierung Beteilig-

ten gehen mit unterschiedlichen Konzepten und daraus folgend jeweils eigener Terminologie ans Werk. Zudem unterliegt der gesamte Bereich einem rasanten Wandel. Im Hinblick auf einen möglichst weit reichenden Einsatz der erarbeiteten datenschutzrechtlichen Handlungsempfehlungen lohnt dennoch der Versuch, die zurzeit wichtigsten Anwendungen des eGovernment in einzelne Kategorien oder Modelle einzuteilen, die sich in Zielrichtung, Auswirkung und den daraus resultierenden Sicherheitsanforderungen deutlich voneinander unterscheiden.

Auf der **Primärebene** der eGovernment-Anwendungen finden sich im Wesentlichen drei zu differenzierende Modelle: **eInformation**, **eKommunikation** und **eTransaktion**. Wegen ihres grundlegenden Charakters lassen sie sich weder einzelnen Verwaltungsaufgaben noch ganz bestimmten Beziehungskonstellationen zuordnen; ihre Einsatzmöglichkeiten gehen prinzipiell sogar über den Bereich der öffentlichen Verwaltung hinaus. Mit Blick auf den Zweck der vorliegenden Broschüre orientiert sich die nachfolgende Beschreibung der Kategorien an ihren jeweiligen Erscheinungsformen im Zusammenhang mit eGovernment-Anwendungen, wobei sich bei dem Modell eTransaktion der im Verwaltungsbereich regelmäßig vorkommende Unterfall des „**e-Verwaltungsverfahren**“ als eigenständige Kategorie herausgebildet hat.



eInformation
eInformation ist das erste und bis heute das am weitesten verbreitete Modell von e-Government. Hierzu gehören neben den klassischen Informationsangeboten insbesondere die zentralen Portale der öffentlichen Verwaltung. Regelmäßig handelt es sich bei eInformation um eine einseitige eGovernment-Komponente. Die jeweiligen Inhalte werden durch die Anbieter unaufgefordert bereitgestellt und von einem unbekannten Nutzerkreis ohne eine darüber hinausgehende Kontaktaufnahme abgeholt.

Weder Anbieter noch Nutzer sind an einer direkten Kommunikation miteinander interessiert. eInformation zieht grundsätzlich keine rechtlich verbindlichen Wirkungen nach sich.

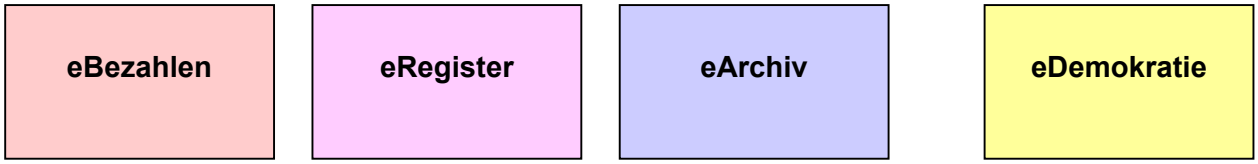
eKommunikation
Inhalt dieses eGovernment-Modells sind Aufbau und Durchführung reiner auf den Austausch von Informationen gerichteter Kommunikationsprozesse. Beispiele hierfür sind Online-Verbindungen, Videokonferenzen oder Internetchats, aber auch die mittlerweile als Standard geltende eMail. Im Gegensatz zu eInformation handelt es sich bei eKommunikation um einen auf Austausch zielenden Kontakt zwischen den Beteiligten, wobei neben der grundsätzlich erwarteten Vertraulichkeit häufig Identifikation und Authentifikation der Teilnehmer bzw. Adressaten von entscheidender Bedeutung sind. eKommunikation ist gleichzeitig ein übergreifend einsetzbares Instrument einer eGovernment-Infrastruktur, bei der die eMail als System der Nachrichtenübermittlung eine besondere Bedeutung hat.

eTransaktion
Die elektronische Realisierung rechtlich verbindlicher Erklärungen der öffentlichen Verwaltung wie z.B. Verwaltungsakte oder Auftragserteilungen ist der bedeutendste Bestandteil dieses eGovernment-Modells. Voraussetzung dafür ist die Nutzung der elektronischen Signatur. Kennzeichnend für eTransaktion sind die rechtlichen Auswirkungen auf die Beteiligten, die entweder in Kombination mit eKommunikation (Übermittlung via eMail) oder auf dem Online-Wege erzeugt werden.

eVerwaltungsverfahren
eVerwaltungsverfahren als Unterfall von eTransaktion umfasst über die eigentliche Transaktion hinausgehend das Vor- und Umfeld von Verwaltungsentscheidungen: den gesamten Workflow innerhalb der Verwaltung, d.h. die elektronische Vorgangsbearbeitung inklusive Formularbereitstellung, Fristenüberwachung, interner Aktenführung und haushaltsmäßiger Abwicklung bis zum Abschluss des Verfahrens unter Einschluss der Rechnungsprüfung. Hierzu gehören auch z.B. die elektronische Gewährung von Akteneinsicht und die Erteilung rechtlich verbindlicher Auskünfte. Schwerpunkt von eVerwaltungsverfahren ist – abgesehen von den unter eTransaktion bereits genannten Aspekten zum rechtlich verbindlichen Abschluss des Verfahrens - die Bereitstellung einer elektronischen Infrastruktur für die medienbruchfreie Durchführung der Verwaltungsabläufe beim eGovernment. Je nach zugrunde liegender Sachaufgabe sind dabei unterschiedliche inhaltliche Anforderungen an die technische Ausgestaltung des jeweiligen Verfahrens zu stellen, so z.B. die Integration mehrerer Verwaltungen in einen Entscheidungsprozess oder die Möglichkeit von Sachstandsabfragen für die am Verfahren Beteiligten.

Die **Sekundärebene** der eGovernment-Anwendungen enthält diverse für die Lösung bestimmter Begleitaufgaben der Verwaltung entwickelte Verfahrensmodelle, die allerdings regelmäßig nicht auf den Einsatz in einem bestimmten Verwaltungsbereich beschränkt sind. Zurzeit lassen sich insoweit drei Erscheinungsformen feststellen: **eBezahlen**, **eRegister** und **eArchiv**. Davon abzugrenzen ist das insbesondere der

Durchführung elektronischer Wahlen auf den verschiedenen Ebenen dienende Modell **eDemokratie**.
In der Zukunft werden sich weitere Modelle auf dieser Ebene herausbilden.



eBezahlen
Im Rahmen der öffentlich-rechtlichen Aufgabenerfüllung haben die Veranlassung von Auszahlungen und die Verbuchung von Zahlungseingängen eine erhebliche Bedeutung. Darüber hinaus gehören zu eBezahlen auf verwaltungsinterner Seite auch die Überwachung von Zahlungsfristen sowie eine Schnittstelle zu dem zugrunde liegenden Verwaltungshaushalt und zur Rechnungsprüfung.

eRegister
Die eGovernment-Anwendung eRegister bezieht sich auf die in der öffentlichen Verwaltung geführten Register und Verzeichnisse, die grundsätzlich einer Fremdnutzung zugänglich sind. Dabei kann der Kreis der in Frage kommenden Nutzer eingeschränkt sein (und eine Authentifizierung erforderlich machen) und/oder von der Zahlung einer Gebühr abhängig sein. Soweit die Nutzung kostenpflichtig ist, muss die Dienstleistung mit dem eGovernment-Modell eBezahlen kombiniert werden. Teilweise zieht die Aufnahme in ein Register oder Verzeichnis auch Rechtswirkungen nach sich (z.B. Grundbuch, Handelsregister), sodass gerade auch hier die Gesichtspunkte der Datensicherheit besonders zu beachten sind.

eArchiv
Kernpunkt von eArchiv ist die elektronische Archivierung abgeschlossener Verfahren. Angesichts der rasanten technischen Entwicklung bei Hardware und Software ist die dauerhafte Nutzbarkeit archivierter elektronischer Dokumente in diesem Zusammenhang ein wesentlicher Gesichtspunkt. Darüber hinaus spielt bei der elektronischen Archivierung aus datenschutzrechtlicher Sicht eine wichtige Rolle, ob einzelne Verfahren oder Arbeitsschritte separat gelöscht werden können.

eDemokratie
Die elektronische Durchführung von Wahlen (einschließlich interner Wahlen der Verwaltung etwa von Personal- oder Schwerbehindertenvertretungen) steht im Mittelpunkt von eDemokratie. Hierzu zählen Vorbereitung, Durchführung und Auswertung der Stimmabgabe. Die Verpflichtung zur Einhaltung der wahlrechtlichen Vorgaben bereitet derzeit für den Praxiseinsatz noch erhebliche Probleme.

2.5 Bewertung der bisherigen Ansätze und Ausblick

Die Entwicklung zum eGovernment ist notwendig und wünschenswert. Der Weg dorthin wird sich jedoch nicht in wenigen Jahren zurücklegen lassen, sondern ein lang anhaltender Lernprozess sein. Umso wichtiger ist es, dass vermehrt öffentliche Dienstleistungen über das Internet angeboten werden, die auch rechtsverbindlich sind und eine tatsächlich spürbare Erleichterung für Bürger und Unternehmen mit sich bringen.

eGovernment und andere gesellschaftliche Formen der Nutzung weltweiter Netze werden zu einem deutlichen Wandel in der Rolle des Staates führen. Immaterialisierung und Globalisierung der Informationsströme durch das Internet führen dazu, dass der Staat dabei Gemeinwohlbelange nicht mehr in dem Umfang durchsetzen und die Grundrechte seiner Bürgerinnen und Bürger nicht so effektiv schützen kann wie bisher. Das gilt insbesondere für das Recht auf informationelle Selbstbestimmung, für dessen Schutz auch der Einzelne selbst tätig werden muss. Die bisherige Vollzugsverantwortung des Staates wird sich also in eine Gewährleistungs- und Infrastrukturverantwortung verändern: Der Staat muss den Einzelnen in die Lage versetzen, die Vertraulichkeit und Integrität seiner personenbezogenen Daten selbst besser als bisher zu schützen, und er muss dazu von seiner Seite die technischen und rechtlichen Rahmenbedingungen schaffen. Dazu gehören der Einsatz von datenschutzfreundlicher Technik ebenso wie die Bereitstellung von Selbstschutzinstrumenten und die Einführung und Förderung von Auditierungsverfahren und Gütesiegeln.

Auf der anderen Seite wird die technische Entwicklung, insbesondere die Erweiterung der Möglichkeiten zur mobilen Datenkommunikation, auch die Strukturen und die Arbeitsverfahren innerhalb der Verwaltungen weiter massiv verändern. Zuständigkeitsgrenzen und Ortsgebundenheit werden ihre Bedeutung verlieren, Produktion und Vertrieb von Verwaltungsleistungen werden getrennt werden können, ganz im Interesse der „Kunden“, die im Sinne eines „One-stop-Government“ ihre unterschiedlichsten Anliegen nur noch über ein einziges Fenster an die Verwaltung herantragen, ohne sich um Zuständigkeiten und Aufgabenverteilungen kümmern zu müssen. Für die politischen Bezüge von Staat und Verwaltung und für die Leistungserstellung und Leistungsabgabe der Verwaltungen werden sich im eGovernment neue Optionen ergeben, die durch Referenzmodelle – unter Einschluss der Anforderungen von Datenschutz und Datensicherheit - frühzeitig erfasst und „kanalisiert“ werden müssen. Für die hier besonders interessierende Schnittstelle Verwaltung/Bürger sind folgende Trends erkennbar:

- Angebote werden zunehmend nach Zielgruppen ausdifferenziert.
- Anwendungen werden sich nicht nur auf wohlstrukturierte, automatisierbare Geschäftsprozesse beschränken, sondern auch komplexere Leistungen erfassen.
- Der Multikanalzugang (Internet-Portal, Call-Center, Bürgerbüro, Brief/Fax, persönlicher Kontakt) zu Angeboten und Anwendungen wird für viele Zielgruppen

die Regel werden, wobei verschiedene Phasen der Interaktion auf unterschiedlichen Kanälen absolviert werden.

- An die Stelle der gegenwärtig zu beobachtenden festen Bündelung von Angeboten (in Lebenslagen) wird eine Öffnung im Sinne eines single-window-Zugangs treten.

- Sicherheitsanforderungen werden stärker auf das im Einzelfall erforderliche Sicherheitsniveau bezogen.

Um Projekte dieses Zuschnitts zu realisieren, werden künftig unterschiedliche staatliche und kommunale Ebenen stärker zusammenarbeiten. In diesem Zusammenhang werden auch Bestrebungen zur Systematisierung und Zentralisierung von gemeinsam nutzbaren Datenbeständen an Bedeutung gewinnen. Die wachsende Dekonzentration der Leistungsabgabe in unterschiedlichen Formen kann mit einer zunehmenden Konzentration der Leistungserstellung einhergehen. Die gegenwärtige Austarierung des Aufgabenbestands zwischen Bund, Ländern und kommunalem Bereich könnte davon nicht unberührt bleiben.

3 eGovernment – Allgemeine Anforderungen

3.1 eGovernment für jedermann

In der Informations- und Wissensgesellschaft hat der gleichmäßige Zugang zu den modernen Informations- und Kommunikationstechnologien und zu den über sie vermittelten Inhalten zentrale Bedeutung für die wirtschaftlichen, gesellschaftlichen und kulturellen Entwicklungs- und Teilhabemöglichkeiten des Einzelnen. Die Nutzung dieser Technologien eröffnet neue Chancen für eine aktive und engagierte Mitwirkung der Bürgerinnen und Bürger an der politischen Willensbildung und an der Herausbildung der öffentlichen Belange auf allen staatlichen Ebenen. Es ist daher eine zentrale politische und gesellschaftliche Aufgabe, die Voraussetzungen für gleiche Zugangs- und Nutzungsmöglichkeiten zu schaffen und die sonst drohende digitale Spaltung der Gesellschaft zu verhindern. Hierfür muss eine leistungsfähige, für alle zugängliche und bedienungsfreundliche technische Infrastruktur (Geräte, Netze, Programme) geschaffen werden. Zugleich muss die Vermittlung von technischer und kultureller Medienkompetenz für jedermann, gerade auch für ältere Menschen, Zuwanderer, sozial Schwache und Behinderte gewährleistet werden.

Zugangs- und Nutzungsmöglichkeiten für jeden zu sichern, ist auch eine Grundanforderung beim eGovernment. Dabei darf aber die Nutzung des elektronischen Weges zu den Verwaltungen nicht rechtlich verpflichtend oder faktisch alternativlos vorgegeben werden. Bestandteil der kommunikativen Autonomie des Einzelnen ist nämlich auch die Möglichkeit, das Medium, in dem man mit der Verwaltung kommunizieren will, grundsätzlich frei wählen zu können. Das bedeutet, dass beim individuellen eGovernment - zumindest derzeit - neben den elektronischen auch noch analoge Handlungsmöglichkeiten bereitgehalten werden müssen.

3.2 Rechtliche und technisch-organisatorische Rahmenbedingungen

Die Einhaltung der rechtlichen und technischen Vorgaben zur Gewährleistung einer rechtsverbindlichen und sicheren elektronischen Kommunikation und Leistungsbeziehung mit den Bürgerinnen und Bürgern sowie mit der Wirtschaft ist eine Grundvoraussetzung für die notwendige Akzeptanz von eGovernment. Dem Datenschutz kommt die Aufgabe zu, die informationelle Selbstbestimmung technikspezifisch und risikoadäquat zu gewährleisten. Dazu ist zunächst herauszuarbeiten, welche Arten von personenbezogenen Daten beim eGovernment anfallen.

3.2.1 Personenbezogene Daten im eGovernment

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Dies sind z.B. Name, Adresse, Eigenschaften einer Person, aber auch Beziehungen zur Umwelt oder Eigentumsverhältnisse. Im eGovernment handelt es sich einerseits um die personenbezogenen Daten, die die öffentlichen Stellen in ihre Angebote einstellen (etwa Name und Funktionsbezeichnung von Mitarbeiterinnen und Mitarbeitern), und andererseits um die Daten von Bürgerinnen und Bürgern, die bei der Kommunikation mit der Verwaltung und bei der Vorgangsbearbeitung zur Erledigung von Verwaltungsaufgaben anfallen.

Das Bundesdatenschutzgesetz und die entsprechenden landesgesetzlichen Regelungen unterscheiden nur zwischen "besonderen Arten personenbezogener Daten", für die besondere Schutzvorschriften gelten, und den übrigen Daten, bei denen ganz bewusst keine weitere Gewichtung vorgenommen wird. Dementsprechend muss für alle personenbezogenen Daten – unabhängig von ihrer Sensibilität oder einer besonderen Schutzwürdigkeit – in jedem Fall zunächst ein Grundschutz gewährleistet sein. Besondere Arten personenbezogener Daten sind gem. der Definition in § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
Daten, die dem Sozialgeheimnis, dem Personalaktengeheimnis oder einem anderen besonderen Amts- oder Berufsgeheimnis unterliegen, sind nach spezialgesetzlichen Regelungen besonders geschützt.

Bei der Nutzung des elektronischen Weges im Rahmen von eGovernment-Anwendungen, also bei der Inanspruchnahme von eMail-Diensten oder Online-Verbindungen zur Verwaltung, handelt es sich rechtlich um die Inanspruchnahme von Telekommunikations- und Tele- oder Mediendiensten (vgl. dazu unter 3.5). Dabei fallen - neben den vorgangsbezogenen Daten der Bürgerin oder des Bürgers - weitere personenbezogene Daten an, die sich in folgende Datentypen einteilen lassen:

Bestandsdaten
Bestandsdaten sind jene personenbezogenen Angaben, die dem Betroffenen auf Dauer zugeordnet sind. Dazu zählen in erster Line die Daten, die für die Nutzung von angebotenen eGovernment-Anwendungen erforderlich sind. Die Definition dieser Daten ist für die Bereiche der Teledienste, Mediendienste und Telekommunikations-

dienste (siehe hierzu auch Abschnitt 3.5) identisch. Dies können sein: Name, Anschrift, eMail-Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, User-ID, statische IP-Adressen und ähnliche Angaben. Welche Bestandsdaten im Einzelnen erhoben, verarbeitet oder genutzt werden dürfen, ist im Wesentlichen abhängig von der technischen Ausgestaltung des Dienstes und von dem Inhalt der jeweiligen eGovernment-Anwendung.

Nutzungsdaten
Nutzungsdaten sind gem. § 6 Abs. 1 TDDSG bzw. § 19 Abs. 2 MDStV Daten, die erforderlich sind, um die Inanspruchnahme von Tele- und Mediendiensten zu ermöglichen und diese abzurechnen. Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Tele- oder Mediendienste.

Verbindungsdaten
Bei Angeboten, die sich auf die reine Übermittlung von Daten beschränken (z.B. e-Mails), handelt es sich um Telekommunikationsdienste. Die bei der Erbringung dieser Dienste anfallenden Daten sind Verbindungsdaten im Sinne des Telekommunikationsrechts (§ 2 Nr. 4 TDSV). Verbindungsdaten bei eMail-Diensten sind insbesondere eMail-Adressen (die auch Bestandsdaten sein können), Zeitpunkte der Sendung bzw. Zustellung und Routing-Informationen (Angaben über diejenigen Rechner, die eine eMail durchgeleitet haben). Nicht zu den Verbindungsdaten gehören Angaben mit Bezug zum Inhalt, also auch Bezeichnungen von Datei-Anlagen und über den Betreff.

Inhaltsdaten
Die Beurteilung der Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung von Inhaltsdaten bei Telekommunikations-, Tele- oder Mediendiensten, also der eigentlichen vorgangsbezogenen personenbezogenen Daten des Bürgers/der Bürgerin, richtet sich nach den Vorschriften des allgemeinen Datenschutzrechts, soweit nicht spezialgesetzliche Regelungen (z.B. die Erhebung von Sozialdaten nach den Vorschriften des Sozialgesetzbuches, Auskünfte zum Meldewesen nach dem Meldegesetz etc.) einschlägig sind. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, ist zusätzlich zu beachten.

Die Frage, ob IP-Nummern personenbezogen sind, ist von großer Bedeutung, weil an verschiedenen Stellen des Internet IP-Adressen - teilweise zusammen mit anderen Nutzungsdaten - protokolliert werden und durch Zusammenführen dieser Daten Profile über das Nutzungsverhalten erstellt werden können. Auf jeden Fall sind statische IP-Adressen personenbezogene Daten, da diese einen direkten und andauernden Bezug zu dem Nutzenden enthalten und auf diesen ohne weiteres rückschließen lassen. Mit Hilfe Dritter ist es darüber hinaus aber bereits jetzt in vielen Fällen möglich, Internet-Nutzer und -Nutzerinnen auch bei nicht-statischen IP-Adressen zu identifizieren. Dynamische IP-Adressen müssen daher ebenfalls als personenbezogene Daten behandelt werden, da sie durch Zusammenführung mit den dahinter stehenden Zu-

ordnungstabellen den Rückschluss auf bestimmbare Personen zulassen (vgl. §§ 3 Abs. 1 BDSG, 1 Abs. 2 TDDSG). Als Folge dieser Zuordnung sind für das Erheben, Verarbeiten, Nutzen und auch Löschen von IP-Adressen die Vorschriften für Verbindungs- bzw. Nutzungsdaten anzuwenden.

Die Frage des Schutzbedarfs personenbezogener Daten ist in den Kapiteln 5.1 und 6.2.1 behandelt.

3.2.2 Rechtliche Rahmenbedingungen

Für den Schutz der personenbezogenen Daten beim eGovernment sind neben den verfassungsrechtlich unverzichtbaren Prinzipien der Erforderlichkeit, der Zweckbindung und der Transparenz die folgenden Leitplanken zu beachten:

3.2.2.1 Zulässigkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten stellt nach der Rechtsprechung des Bundesverfassungsgerichts einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, der einer ausdrücklichen gesetzlichen Erlaubnis oder einer Einwilligung des Betroffenen bedarf. Zu den Rechtsvorschriften, aus denen sich eine Erlaubnis für eine Datenverarbeitung ergeben kann, zählen neben Gesetzen und Rechtsverordnungen auch Satzungen, die von einer juristischen Person des öffentlichen Rechts im Rahmen der ihr verliehenen Autonomie erlassen werden, sowie allgemein verbindliche tarifvertragliche Regelungen und Dienstvereinbarungen zwischen Dienststelle und Personalvertretungen.
Fehlt eine einschlägige Rechtsvorschrift, darf die Datenverarbeitung nur mit vorheriger Zustimmung des Betroffenen erfolgen (Einwilligung). Die Einwilligung muss auf der freien Willensentscheidung des Betroffenen beruhen. Die Freiwilligkeit ist grundsätzlich dann zu verneinen, wenn aufgrund rechtlicher oder faktischer Abhängigkeiten die Entscheidungsmöglichkeiten des Betroffenen wesentlich eingeschränkt sind. Die Einwilligung muss hinreichend bestimmt sein. Zum Zeitpunkt der Abgabe der Erklärung müssen die verantwortliche Stelle, die Art der zu verarbeitenden Daten, der Umfang, die Form und der Zweck der Verarbeitung, mögliche Verknüpfungen mit anderen Datenbeständen sowie bei beabsichtigter Datenübermittlung auch die künftigen Datenempfänger für den Einwilligenden eindeutig erkennbar sein. Eine unterlassene oder unvollständige Aufklärung führt zu einer Unwirksamkeit der Einwilligung. Bei besonders sensiblen Daten (§ 3 Abs. 9 BDSG) muss die Einwilligung sich ausdrücklich auf diese Daten beziehen.
Über die Bedeutung der Einwilligung muss der Betroffene umfassend aufgeklärt werden, damit er Inhalt und Tragweite seiner Erklärung überblicken kann. Zur Aufklärung gehört auch ein Hinweis darauf, dass die Einwilligung verweigert oder mit Wirkung für die Zukunft widerrufen werden kann. Die jeweiligen Rechtsfolgen dieses Verhaltens sind darzustellen. Ein Widerruf für die Vergangenheit kommt nicht in Betracht, da Datenverarbeitungen, die aufgrund einer ursprünglich erteilten Einwilligung durchgeführt worden sind, nicht nachträglich die Rechtsgrundlage entzogen werden kann.
Sofern im Rahmen einer eGoverment-Anwendung die Möglichkeit einer elektronischen Einwilligung angeboten wird, ist dafür § 4 TDDSG zu beachten, d.h. die Einwilligungserklärung muss durch eine eindeutige und bewusste Handlung des Nutzers

erfolgen, sie muss protokolliert werden und jederzeit abrufbar sein. Das Angebot zur elektronischen Einwilligung muss außerdem einen Hinweis auf die Widerrufbarkeit der Einwilligung enthalten und das Koppelungsverbot beachten.

3.2.2.2 Erforderlichkeit

Eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur erforderlich, wenn die jeweilige Aufgabe ohne das konkrete Datum nicht oder nicht vollständig erfüllt werden kann. Dazu zählt auch, dass die Aufgabe auf andere Weise nur unter unverhältnismäßig großen Schwierigkeiten, mit einem unvertretbar höheren Aufwand oder verspätet erfüllt werden könnte. Eine Datenerhebung „auf Vorrat“ ist unzulässig. Die Erforderlichkeit setzt die Geeignetheit voraus, das heißt Daten, die zur Erreichung des Verarbeitungszieles überhaupt nicht geeignet sind, sind schon von daher auch nicht erforderlich. Insbesondere ist von der Möglichkeit der Anonymisierung und Pseudonymisierung Gebrauch zu machen. Systemseitig sind Vorkehrungen zu treffen, dass die Daten zum frühestmöglichen Zeitpunkt gelöscht oder zumindest der Personenbezug durch Anonymisierung aufgehoben oder durch Pseudonymisierung gelockert werden kann.

3.2.2.3 Datenvermeidung und Datensparsamkeit

Der Grundsatz der Datenvermeidung und Datensparsamkeit gebietet, schon im Vorfeld bei der Entwicklung und Auswahl von Datenverarbeitungssystemen und bei der Ausgestaltung der konkreten Datenverarbeitungsprozesse darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden. Er gibt damit ein allgemeines Gestaltungsprinzip vor, das das Entstehen von Daten mit Personenbezug oder Personenbeziehbarkeit von vornherein ausschließen oder auf ein Minimum beschränken will. Dies ist Ausdruck eines erweiterten Verständnisses von Datenschutz, das den Grundsatz der Verhältnismäßigkeit für die Datenverarbeitung einzelfallübergreifend mit Handlungsvorgaben für die System- und Verfahrensausgestaltung konkretisiert.
Die Regelung ist vom Erforderlichkeitsprinzip abzugrenzen; die Erforderlichkeit als materiell-rechtliche Anforderung beschränkt nur den Umfang der Datenverarbeitung im Einzelfall.

3.2.2.4 Zweckbindung

Das Gebot der Zweckbindung soll sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind (Zweckidentität). Der Zweck der Datenverarbeitung folgt aus der jeweiligen Fachaufgabe, zu deren Erfüllung die Daten erhoben wurden. Sofern Daten der öffentlichen Stelle ohne Erhebung zur Kenntnis gelangt sind, legt sie den Zweck bei der erstmaligen Speicherung fest. Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck ist als Zweckänderung oder Zweckdurchbrechung nur auf gesetzlicher Grundlage oder dann zulässig, wenn der Betroffene eingewilligt hat. Dies gilt auch dann, wenn die Daten innerhalb der Behörde an eine andere Stelle mit einer anderen, über bloße Hilfsfunktionen hinausgehenden Aufgabenstellung weitergegeben werden sollen; denn die öffentliche Verwaltung stellt keine Informationseinheit dar, es gilt der Grundsatz der informationellen Gewaltenteilung. Eine verstärkte Zweckbindung besteht für Daten,

die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Ein striktes Verbot der Zweckänderung besteht für Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

Die Europäische Datenschutzrichtlinie lässt in Art. 6 Abs. 1 b an Stelle der Zweckidentität eine Zweckvereinbarkeit zu. Ob für bestimmte Ausgestaltungen des eGovernment (zum Beispiel Wissensmanagement, multifunktionale Serviceangebote) de lege ferenda auch eine Lösung vertretbar wäre, die bei einer Zweckvereinbarkeit eine anderweitige Verarbeitung jedenfalls dann zulässig macht, wenn der Betroffene nicht widersprochen hat, muss bei der zweiten Stufe der Modernisierung der Datenschutzrechts-Novellierung beantwortet werden.

3.2.2.5 Transparenz

Das informationelle Selbstbestimmungsrecht für Betroffene setzt Kenntnis über die Struktur der Datenverarbeitung, über die Datenverarbeitungsprozesse, über die eingesetzte Technik und über die Datenströme voraus. Jede eGovernment-Anwendung muss die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten und über die Daten verarbeitenden Stellen informieren. Nur wenn die Betroffenen erfahren, welche personenbezogenen Daten über sie für welche Zwecke erhoben werden, wie die Struktur der Datenverarbeitung aussieht und wie die Datenverarbeitungsprozesse ablaufen und wer dafür die Verantwortung trägt, haben sie auch die Möglichkeit, ihre individuellen Rechte wahrzunehmen. Das Transparenzgebot wird gewährleistet durch

- Hinweispflichten über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten,
- durch Unterrichtungspflichten über die Möglichkeit anonymen und pseudonymen Handelns, über Profilbildungen,
- durch Informationspflichten über die Identität der verantwortlichen Stelle (Anbieterkennzeichnung, Impressum) und über die Auskunftsansprüche der Betroffenen. Diese Informationen sollten in einer Datenschutzerklärung zusammengefasst werden.

3.2.2.6 Korrekturrechte der Betroffenen

Zu den Korrekturrechten der Betroffenen gehört der Anspruch auf Berichtigung, Löschung und Sperrung der zu ihrer Person gespeicherten Daten. Unrichtige Daten beeinträchtigen das Recht auf informationelle Selbstbestimmung genauso wie unrechtmäßig erhobene Daten und sind daher unverzüglich zu berichtigen. Die Pflicht zur Berichtigung besteht unabhängig davon, ob der Betroffene einen Anspruch geltend macht.

Die speichernde Stelle hat die Daten zu löschen, wenn die Speicherung nicht zulässig oder für die Aufgabenerfüllung nicht mehr erforderlich ist. Dabei bedeutet Löschen das Unkenntlichmachen von Daten, sodass sie für niemanden mehr zugänglich sind. Die Löschung hat unverzüglich, d.h. ohne schuldhaftes Zögern, zu erfolgen. Wenn Aufbewahrungspflichten bestehen oder wenn anzunehmen ist, dass schutzwürdige

Interessen des Betroffenen durch die Löschung beeinträchtigt werden, tritt an die Stelle der Löschung eine Sperrung.

Daten sind außerdem zu sperren, wenn ihre Richtigkeit nicht eindeutig ist oder die Sperrung von dem Betroffenen verlangt wird. Darüber hinaus haben Betroffene die Möglichkeit, einer an sich rechtmäßigen Datenverarbeitung aus besonderen schutzwürdigen persönlichen Gründen zu widersprechen. Der Widerspruch zwingt die verantwortliche Stelle, die beabsichtigte Datenverarbeitung im Hinblick auf die vom Betroffenen geltend gemachte besondere persönliche Situation zu überprüfen.

3.2.2.7 Automatisierte Einzelentscheidungen

Die Vorschrift des § 6a BDSG soll gewährleisten, dass Entscheidungen, bei denen eine Bewertung von Persönlichkeitsmerkmalen vorgenommen wird, nicht ausschließlich durch eine technische Vorrichtung getroffen, sondern immer von einem Menschen verantwortet werden. Bei den Persönlichkeitsmerkmalen muss es sich um Angaben von einer gewissen Komplexität handeln; bloße Messwerte (wie die Angabe des Blutalkoholgehalts) reichen nicht aus. Beispiele für die angesprochenen Persönlichkeitsmerkmale sind die berufliche Leistungsfähigkeit, die Zuverlässigkeit oder das Verhalten einer Person. Den Einsatz automatisierter Datenverarbeitung zur Vorbereitung oder Unterstützung einer Entscheidung, die sich auf entsprechende Persönlichkeitsmerkmale bezieht, schließt die Vorschrift nicht aus. Eine Vorauswahl geeigneter Personen nach bestimmten Kriterien ist deshalb im Wege der automatisierten Datenverarbeitung durchaus möglich. Ausschlaggebend ist, dass die abschließende Entscheidung von einer Person verantwortet wird. Zulässig ist eine automatisierte Einzelentscheidung allerdings, wenn die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstiges Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder die Wahrung der berechtigten Interesse des Betroffenen durch geieignete Maßnahmen gewährleistet wird.

3.2.3 Technische und organisatorische Sicherungen

Das Recht auf informationelle Selbstbestimmung verlangt neben dem rechtlichen Schutz der personenbezogenen Daten eine angemessene Datensicherheit. Gestaltungsziele der informationstechnischen Sicherheit sind Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Transparenz und Revisionsfähigkeit. Die Sicherungsziele sind Technologie unabhängig. Für jede eGovernment-Anwendung sind die folgenden Gestaltungsanforderungen im Rahmen eines Sicherheitskonzeptes konkret auszufüllen.

3.2.3.1 Vertraulichkeit und Integrität

Die Übermittlung der Daten im Internet ohne technische Schutzvorkehrungen ähnelt einer mit Bleistift in Druckbuchstaben geschriebenen Postkarte. Der Inhalt kann von Dritten eingesehen und ohne Kenntnis des Absenders oder Adressaten verändert werden. In der analogen Papierwelt sind Änderungen in aller Regel nachvollziehbar, in der elektronischen Welt ist es ohne geeignete Gegenmaßnahmen möglich, die elektronischen Inhalte einzusehen und unbemerkt zu verändern.

Die nachfolgenden Fragen verdeutlichen den Bedarf an besonderen Sicherungen für die Vertraulichkeit und Integrität:

- Werden personenbezogene Daten verarbeitet?
- Welche Folgen hat es, wenn gespeicherte Daten in falsche Hände geraten?
- Für welche Daten ist es besonders kritisch, wenn sie verfälscht werden?
- Welche Folgen hat es, wenn unbemerkt mit verfälschten Daten weitergearbeitet wird?

Der Schutzbedarf ist pauschal umso höher anzusetzen, je größer der potentielle Schaden ist und je später der Schaden bemerkt werden kann.

3.2.3.2 Verfügbarkeit

Verfügbarkeit für eGovernment-Anwendungen ist gewährleistet, wenn die personenbezogenen Daten zeitgerecht und ordnungsgemäß verarbeitet werden können. Kritisch wird es, wenn Daten verloren gehen oder technische Defekte Rechner und Daten beeinträchtigen. Zur Feststellung der Anforderungen an die Verfügbarkeit sind folgende Fragen zu klären:

- Wie lange kann höchstenfalls auf den Rechner bzw. die Daten verzichtet werden (Stunden, Tage oder Wochen)?
- Welcher Termin ist der kritischste für den Ausfall des Rechners oder den Verlust der Daten?
- Welche Folgen hat ein längerfristiger Rechnerausfall?
- Welcher Schaden tritt ein, wenn Daten endgültig verloren sind?
- Wie lange dauert es und wie viel kostet es, das System wiederherzustellen oder die Daten erneut zu erfassen?

3.2.3.3 Authentizität

Personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können. Dabei ist zu unterscheiden zwischen dem Identitätsnachweis (die Kommunikationspartner weisen sich zweifelsfrei aus) und dem Herkunftsnachweis (der Absender weist nach, dass eine Nachricht von ihm stammt und nicht verändert wurde). Mit der Authentisierung sollen unberechtigte Zugriffe erkannt und abgewehrt werden sowie sensible Daten bei der Übertragung über Netze geschützt bleiben. Dazu sind Verfahren erforderlich, die allen Beteiligten die Feststellung der Identität ihrer Kommunikationspartner unmissverständlich ermöglichen.

3.2.3.4 Revisionsfähigkeit

Verantwortliche Stellen sind auch bei eGovernment-Anwendungen verpflichtet, technische und organisatorische Maßnahmen zu treffen, damit nachträglich überprüft und festgestellt werden kann, wer welche personenbezogenen Daten zu welcher Zeit eingegeben bzw. übermittelt hat. Auch Versuche missbräuchlicher Verarbeitung müssen nachträglich untersucht werden können. Mit einer Protokollierung wird einer missbräuchlichen Verwendung personenbezogener Daten vorgebeugt, weil keiner darauf vertrauen kann, dass Verstöße unentdeckt bleiben. Mit der Protokollierung entstehen allerdings besondere Sammlungen personenbezogener Daten über Nutzerinnen und Nutzer. Daraus lassen sich Nutzerprofile ableiten oder Listen über Auffälligkeiten erstellen. Das Datenschutzrecht lässt das jedoch ohne Einwilligung der Betroffenen

grundsätzlich nicht zu. Protokolldaten dürfen nur zu Zwecken genutzt werden, die Anlass für ihre Speicherung waren, und dürfen nicht für andere Zwecke verarbeitet werden. Nach beamtenrechtlichen Regelungen (zum Beispiel § 101 Abs. 6 Niedersächsisches Beamtengesetz) wird die Verwendung von Protokolldaten zu Zwecken der Verhaltens- und Leistungskontrolle untersagt. Im Einzelfall ist eine Auswertung der Protokolldaten zur Aufdeckung von Missbräuchen zulässig. Die Zweckbindung der Protokollierung muss daher technisch und organisatorisch sichergestellt werden. Der Grundkonflikt, der sich bei jeder Protokollierung mit dem Prinzip der Datenvermeidung und Datensparsamkeit ergibt, kann nur im Einzelfall gelöst werden.

3.3 Ergänzende Datenschutzanforderungen

Die dargestellten Sicherungen sollten beim eGovernment um weitere Maßnahmen ergänzt werden.

3.3.1 Risikoabschätzung durch Vorabkontrolle

Öffentliche Stellen des Bundes und der Länder haben grundsätzlich vor Einführung einer eGovernment-Anwendung zu prüfen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen wirksam beherrscht werden können. Die Risikoabschätzung dient dazu, die Abläufe der automatisierten Datenverarbeitung transparent zu machen, Gefahren für die Rechte der betroffenen Bürgerinnen und Bürger aufzuzeigen, Sicherungsmaßnahmen zu entwickeln und Restrisiken abzuschätzen, um im Ergebnis einen datenschutzgerechten Technikeinsatz zu erreichen. Eine Risikoabschätzung ist insbesondere dann durchzuführen, wenn sensitive personenbezogene Daten (§ 3 Abs. 9 BDSG) verarbeitet werden oder die Verarbeitung dazu bestimmt ist, die Persönlichkeit Betroffener zu bewerten einschließlich seiner Fähigkeit, seiner Leistung oder seines Verhaltens. eGovernment-Verfahren dürfen nur eingesetzt werden, soweit derartige Gefahren durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

3.3.2 Datenschutzmanagement

Datenschutzgerechtes eGovernment erfordert klare Festlegungen, wer für welche Aufgaben verantwortlich ist und wer die Verantwortung für die Vollständigkeit und Korrektheit von Daten und Verfahren trägt. Hierfür ist ein Datenschutzmanagement zu schaffen und zu veröffentlichen. Alle verfahrensmäßigen und technisch-organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit müssen konsequent umgesetzt und in ihren Wirkungen im Rahmen eines begleitenden Controllings intensiv beobachtet werden. Nur so ist sichergestellt, dass die Effektivität der Maßnahmen gewährleistet bleibt, Fehlentwicklungen oder Vollzugsdefizite frühzeitig entdeckt und notwendige Weiterentwicklungen zeitgerecht eingeleitet werden können. Dies ist primär Aufgabe der behördlichen Datenschutzbeauftragten. Sie können in Fragen des Datenschutzes und der Datensicherheit die Hilfe der oder des staatlichen Beauftragten für den Datenschutz in Anspruch nehmen.

3.3.3 Ausreichende Qualifizierung

Unerlässliche Voraussetzung für ein funktionierendes eGovernment ist die systematische Schulung der Mitarbeiterinnen und Mitarbeiter und deren Personalvertretung mit

der Vermittlung von Grundlagen über die eingesetzten Verfahren, deren Technikkonzept sowie über die anzuwendenden Datenschutzvorschriften. Die erforderlichen Maßnahmen sind in einem Schulungskonzept zusammenzufassen.

3.3.4 Selbstdatenschutz

Da die Verwaltungen in globalen Netzen nur begrenzt in der Lage sind, die informationelle Selbstbestimmung ihrer Nutzer umfassend zu schützen, ist es erforderlich, dass nach Ausschöpfen aller bereits genannten Sicherungsmöglichkeiten dem Bürger ermöglicht wird, eigene Mittel zum Schutz seiner informationellen Selbstbestimmung zu ergreifen und zu nutzen. Für einen umfassenden Persönlichkeitsschutz sollten dem Nutzer die technischen Instrumente sowie notwendige Infrastrukturleistungen zur Verfügung gestellt werden. Wichtige Mittel des Selbstdatenschutzes sind die selbstbestimmte Nutzung von Anonymitätstechniken, von Pseudonymen oder von Verschlüsselungstechniken. Ein weiteres Instrument des Selbstdatenschutzes ist die Möglichkeit, sich durch Zugriff auf die Datenschutzerklärung der Daten verarbeitenden Stelle jederzeit ausreichende Gewissheit über die Bedingungen und Strukturen der Datenverarbeitung zu verschaffen. Dass die Verwaltung damit ihre Datenverarbeitungspraxis ausdrücklich offen legt, kann dem Nutzer einen Teil seiner Besorgnis nehmen.

3.4 Datenverarbeitung durch Dritte - Auftragsdatenverarbeitung und Funktionsübertragung

Immer häufiger übertragen Verwaltungen einzelne Arbeitsabläufe oder ganze Aufgaben auf andere Stellen (Outsourcing). Dies wirft die Frage auf, wie dieser Vorgang datenschutzrechtlich zu bewerten ist, insbesondere welche Voraussetzungen für eine rechtmäßige Übertragung vorliegen müssen und ob es Grenzen für eine derartige Übertragung gibt.

Das Datenschutzrecht unterscheidet hierzu zwischen Datenverarbeitung im Auftrag und der Funktionsübertragung. Bei der Auftragsdatenverarbeitung liegt die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der personenbezogenen Daten beim Auftraggeber, der „Herr“ seiner Daten bleibt. Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragnehmer vor. Dem Auftragnehmer wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter materieller Verantwortung des Auftraggebers, gewissermaßen als sein verlängerter Arm, übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine „Hilfsfunktion“ der eigentlichen Aufgabe ausgelagert, ohne dass der Auftragnehmer einen eigenen Handlungs- oder Entscheidungsspielraum hat.

Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Auftragnehmer über die technische Durchführung hinaus materielle Leistungen mit Hilfe der überlassenen Daten oder bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Aufgabe, liegt eine Funktionsübertragung vor. In diesem Fall wird der Auftragnehmer zur Daten verarbeitenden Stelle und hat eigenständig für die zur Datensiche-

rung und zur Gewährleistung von Vertraulichkeit erforderlichen technischen und organisatorischen Maßnahmen zu sorgen.

Die Bewertung, ob eine Auftragsdatenverarbeitung oder Funktionsübertragung vorliegt, lässt sich nur im Einzelfall vornehmen. Deutliche Erkennungsmerkmale bei Auftragsdatenverarbeitung sind die fehlende Entscheidungsbefugnis des Dritten, die weisungsgebundene Unterstützungstätigkeit und die fehlende Beziehung des Dritten zum Betroffenen. Merkmale der Funktionsübertragung sind weiterhin die Überlassung von Nutzungsrechten an den Daten, die eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dritten sowie das Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch).

Besondere Probleme ergeben sich bei Daten, für die besondere Schutzvorschriften bestehen. Durch die Datenweitergabe werden die Daten dem Dritten offenbart. Dies ist unzulässig, wenn der Offenbarung gesetzliche Schutzvorschriften entgegenstehen. Dazu gehören insbesondere Berufsgeheimnisse (zum Beispiel das Arztgeheimnis) und besondere Amtsgeheimnisse (wie das Steuergeheimnis). In diesen Fällen ist eine Weitergabe der Daten an Dritte nur zulässig, wenn die betreffenden Schutzvorschriften die Offenbarung dieser Daten erlauben. Zur Zusammenarbeit mit Dritten und den dabei erforderlichen technischen und organisatorischen Maßnahmen finden Sie u.a. in den folgenden Kapiteln weitere Hinweise:

- Kapitel 5.2 Erforderlichkeit
- Kapitel 5.7.6 Zahlungsverfahren
- Kapitel 5.7.9 Einschaltung Dritter
- Kapitel 6.1.5 Schutz des Web-Angebotes und der Infrastruktur
- Kapitel 6.2.4 Technische Ausgestaltung von Auftragsverhältnissen

3.5 Zusammenspiel der gesetzlichen Grundlagen

Beim eGovernment werden die Möglichkeiten der elektronischen Kommunikation über das Internet genutzt. Dabei können Daten an einem Ort erhoben, an einem anderen Ort gespeichert und an einem dritten Ort genutzt werden. Hierfür gibt es keine verbindlichen internationalen Datenschutz-Standards, gleichwohl werden von den meisten Beteiligten im Internet einige Grundregeln freiwillig beachtet.
In der Bundesrepublik Deutschland sind hierfür komplexe rechtliche Rahmenbedingungen geschaffen worden, die insbesondere den Umgang mit den bei der elektronischen Kommunikation anfallenden Bestands-, Verbindungs-, Nutzungs- und Inhaltsdaten (vgl. dazu oben unter 3.2.1) regeln. Bei Einrichtung und Betrieb von Internet-Diensten sind im Einzelnen folgende Datenschutz-Vorschriften zu beachten:

- für die erste Ebene: das Telekommunikationsgesetz (TKG) und die Telekommunikationsdatenschutzverordnung (TDSV),
- für die zweite Ebene: das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) sowie der Mediendienstestaatsvertrag (MDStV),
- für die dritte Ebene: die allgemeinen Datenschutzvorschriften im Bundesdatenschutzgesetz, in den Datenschutzgesetzen der Länder sowie in anderen bereichsspezifischen Gesetzen.

Dabei gilt auf der zweiten Ebene für Anwendungen, die auf eine individuelle Nutzung ausgerichtet sind, das Teledienstegesetz und das Teledienstdatenschutzgesetz. Darunter fallen z.B. die elektronische Anforderung von Antragsunterlagen (Wahlunterlagen, Bauanträge), elektronische Bestellverfahren (Müllsäcke, Sperrmüllabfuhr), Gästebücher, Telearbeit etc. Elektronische Informations- und Kommunikationsdienste, die sich an die Allgemeinheit richten, fallen dagegen unter das Medienrecht. Dazu gehören insbesondere Informationsangebote und Abrufdienste mit redaktioneller Gestaltung, wie z.B. der Pressespiegel.
Die drei Ebenen umfassen die folgenden Regelungs-Schichten:

Ebene	Wesentliche Forderungen	Beispiel
Ebene 1: Transportebene **Rechtsgrundlage:** Telekommunikationsrecht (TKG, TDSV)	Fernmeldegeheimnis; Technische Schutzmaßnahmen; Umgang mit Bestands-, Verbindungs- und Abrechungsdaten.	Netzbetrieb; Zugang zum Internet
Ebene 2: Transportbehälterebene **Rechtsgrundlage:** „Online-Recht“ (Teledienstdatenschutzgesetz, Mediendienste-Staatsvertrag)	Informations- und Kennzeichnungspflichten; Verantwortlichkeiten für die angebotenen Informationen; Umgang mit Bestands-, vorgangsbezogenen Nutzungs- und Abrechnungsdaten; Widerspruchsrechte; elektronische Einwilligung.	Nutzung eines Webangebotes
Ebene 3: Inhaltsebene **Rechtsgrundlage:** „Offline-Recht“ BDSG, Landesdatenschutzgesetze	ergeben sich aus dem Fachrecht und den jeweiligen Datenschutzgesetzen	Melderegisterauskunft; Anforderung von Briefwahlunterlagen; Anwohnerparkausweis

Ebene 1: Transportebene

Damit ein Tele- oder Mediendienst angeboten und ein Nutzer ihn in Anspruch nehmen kann, muss eine technische Verbindung zwischen Anbieter und Nutzer hergestellt werden. Hierzu bedient man sich der Dienste eines Telekommunikationsdiensteanbieters. Bei der Bereitstellung der notwendigen TK-Dienste fallen beim TK-Diensteanbieter Bestands-, Verbindungs- und Abrechnungsdaten an. Beim Umgang mit diesen Daten hat der TK-Diensteanbieter das TKG (§§ 85 und 89) und die TDSV zu beachten.

Ebene 2: Transportbehälterebene

Greift nunmehr der Nutzer unter Verwendung der Telekommunikationsverbindung auf das Angebot des Tele- oder Mediendiensteanbieters zu, wird die zweite Schicht, nämlich die Transportbehälterebene berührt. Der Tele- bzw. der Mediendiensteanbieter benötigt für das Bereitstellen seines Dienstes vom Nutzer eine Reihe von personenbeziehbaren Daten und erhebt weitere Daten im Zusammenhang mit der Nutzung des Dienstes. Es fallen also Bestands-, vorgangsbezogene Nutzungs- und Abrechnungsdaten des Nutzers an. Der rechtmäßige Umgang mit diesen Daten und die Rechte der Nutzer sind im TDG, im TDDSG und im MDStV geregelt.

Ebene 3: Inhaltsebene

Wenn ein Tele- oder Mediendienst genutzt wird, werden hierbei Informationen und vielfach auch personenbezogene Daten an den Nutzer weitergegeben oder ausgetauscht. Der Nachrichteninhalt ist in einer eigenen Schicht mit vielfältigen Rechtsvorschriften geregelt. Für den Inhalt der Kommunikation sind die Telekommunikation und die Tele- und Mediendienste nur „Trägermedien“. Zunächst gilt entsprechend dem Gegenstand der betreffenden eGovernment-Anwendung das jeweilige Fachrecht (Inhaltsebene = Offline-Recht); so gilt zum Beispiel für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten bei einer elektronischen Melderegisterauskunft das jeweilige Landesmelderecht. Soweit das Fachrecht keine bereichsspezifischen Regelungen zum Datenschutz enthält, gelten die Regelungen des jeweiligen Landesdatenschutzgesetzes.

Diese Dreiteilung bei den anzuwendenden Datenschutzregelungen, anhand derer die Konkretisierung der jeweils einschlägigen datenschutzrechtlichen Anforderungen vorzunehmen ist, gilt entsprechend bei allen eGovernment-Anwendungen.

Die Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten, die der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bund und der Länder erstellt hat, bietet eine wertvolle Hilfe durch das komplexe Tele- und Medienrecht (www.lfd.niedersachsen.de). Sie erläutert insbesondere die Pflichten der Anbieter.

3.6 Elektronische Signatur

Viele Verwaltungsleistungen werden nur dann erbracht, wenn die Bürger und Unternehmen mit rechtsverbindlichen Unterschriften ihre Identität und ihre Willensbekundung nachweisen. Um ein Verwaltungsverfahren in diesen Fällen vollständig elektronisch abwickeln zu können, ist es daher notwendig, eine elektronische Unterschrift einzusetzten, die rechtlich der eigenhändigen Unterschrift gleichgestellt ist.

Rechtlicher Rahmen für die elektronische Signatur

Für die Anwendbarkeit elektronischer Signaturverfahren für das eGovernment ist neben der Bereitstellung geeigneter technischer Verfahren auch die Bereitschaft der Behörden sicherzustellen, dass elektronische Signaturen anerkannt werden. Das Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) vom 22.05.2001 setzt den Rahmen, in dem elektronische Signaturen im Vergleich zur eigenhändigen Unterschrift als hinreichend sicher angesehen werden. Die Vorgaben werden durch

die Signaturverordnung vom 16.11.2001 (SigV) konkretisiert. Genauere Festlegungen, wann elektronische Signaturen der handschriftlichen Unterschrift gleichgestellt sind, trifft für den privatwirtschaftlichen Bereich das Gesetz zur Anpassung der Formvorschrifften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 01.08.2001 (§ 126a BGB) und für den öffentlichen Bereich das 3. Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 21.08.2002, das in seinen wesentlichen Teilen zum 01.02.2003 in Kraft tritt. Die zentrale Anforderung an eine elektronische Signatur ist die Fälschungssicherheit, also die Gewährleistung, dass die Signatur eines Dokuments durch die Person erfolgt ist, der die Signatur tatsächlich zugeordnet ist. Eine Fälschung der elektronischen Signatur soll möglichst ausgeschlossen sein. Dies ist auch deshalb von besonderer Bedeutung, weil bei der elektronischen Signatur eine Fälschung nicht erkennbar ist, anders als bei der handschriftlichen Unterschrift, bei der Experten in der Regel Fälschungen nachweisen können.

Weitere Anforderungen sind:

- **langfristige Prüfbarkeit**, d. h. auch nach vielen Jahren sollte die Gültigkeit einer Signatur noch online nachprüfbar sein;

- **breite Anwendbarkeit**, d. h. die Signatur sollte bei vielen, idealer Weise sogar bei allen eGovernment-Anwendungen, die eine Signatur fordern, anwendbar sein; auch die Anwendung im privaten Geschäftsverkehr oder im Ausland sollte möglich sein.

Gesetzlich vorgesehene Varianten der elektronischen Signatur
Das Signaturgesetz (SigG) versteht unter elektronischen Signaturen „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Dazu würde es z.B. genügen, einem elektronischen Dokument bzw. einer Willenbekundung den Namen oder die eingescannte Unterschrift des Bekundenden anzufügen. Eine solche elektronische Signatur ist aber nicht gegen Fälschungen geschützt, da sie beliebig kopiert und anderen Dokumenten angefügt werden kann. Etwas höheren Sicherheitsanforderungen genügen die fortgeschrittenen elektronischen Signaturen, mit denen die Identität des Unterzeichners bestätigt und geprüft werden kann, ob das unterschriebene Dokument nachträglich verändert worden ist, ohne dass aber z.B. Anforderungen an das Verfahren der Identifizierung und der Übergabe der Signaturkarte an die richtige Person bestehen. Noch höheren Ansprüchen genügt die qualifizierte elektronische Signatur. Zusätzlich zu den Anforderungen einer fortgeschrittenen Signatur bedarf sie eines zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikats. Außerdem muss ihre Erzeugung besonderen, im SigG näher beschriebenen Sicherheitsanforderungen entsprechen. Die Zertifikate sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet und die Identität dieser Person bestätigt wird. Die Zertifikate gelten als qualifiziert, wenn sie den inhaltlichen Anforderungen des SigG genügen und von Zertifizierungsdiensteanbietern ausgestellt werden, die ebenfalls besonderen gesetzlichen Ansprüchen aus dem SigG genügen müssen. Durch diese Anforderungen soll z.B. die Vertrauenswürdigkeit der Identifizierung und der

Kartenübergabe sichergestellt werden. Zertifizierungsanbieter benötigen für ihre Tätigkeit keine Genehmigung, müssen ihre Tätigkeit jedoch bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) anzeigen. Auf Antrag können sich die Zertifizierungsanbieter bei der RegTP akkreditieren lassen. Dazu ist von einer Bestätigungsstelle zu prüfen, ob der Zertifizierungsanbieter alle Anforderungen des SigG und der SigV erfüllt. Qualifizierte elektronische Signaturen mit Anbieterakkreditierung stellen somit einen Sonderfall der qualifizierten elektronischen Signatur dar, der die höchsten Anforderungen erfüllt. Solche Zertifikate müssen noch 30 Jahre nach Ende der Gültigkeit online prüfbar sein. Dies wird durch die Regulierungsbehörde auch dann sichergestellt, wenn der akkreditierte Anbieter seine Tätigkeit inzwischen eingestellt hat.
Derzeit besteht die Tendenz, sich aus Kostengründen mit unterschiedlichen Varianten fortgeschrittener elektronischer Signatur zu begnügen. Die Signaturen werden dabei entweder nicht oder durch einen lokal bestimmten Zertifizierungsanbieter zertifiziert. Solche Signaturen können auch deshalb die Anforderung als Ersatz der Schriftform nicht erfüllen, weil ihr Anwendungsbereich sachlich und lokal begrenzt ist (z.B. auf eine Universität, ein großes Unternehmen oder eine bestimmte eGovernment-Anwendung). Die Herausbildung einer bundesweit einheitlichen und über die Grenzen wirkenden Signaturinfrastruktur für den gesamten elektronischen Rechts- und Geschäftsverkehr wäre jedoch wünschenswert.

Datenschutzrechtliche Bewertung
Die elektronische Signatur stellt die wichtigste technisch-organisatorische Maßnahme zur Sicherstellung der Authentizität und Integrität für elektronische Daten dar, die im elektronischen Rechts- und Geschäftsverkehr ausgetauscht werden. Unabhängig von der gewählten Variante nach dem SigG ist der bedeutendste Risikofaktor die Erhaltung der Vertraulichkeit des Signaturschlüssels. Dieser Schlüssel wird in der Regel auf einer Chipkarte gespeichert, die im Besitz des Unterzeichners (z. B. Bürgerkarte) und durch eine PIN geschützt ist, die nur dem Unterzeichner bekannt ist. Die Authentizität des Unterzeichners beruht also auf Besitz (der Chipkarte) und Wissen (der PIN), also in gleicher Weise wie auch der Schutz von Kredit- oder Scheckkarten erfolgt. Wann biometrische Verfahren hier ergänzende Sicherheit bieten können, hängt von der weiteren Entwicklung dieser Technologien ab.

3.7 Informationsfreiheit im Rahmen von eGovernment-Anwendungen

Mit Brandenburg, Berlin, Schleswig-Holstein und Nordrhein-Westfalen verfügen inzwischen vier Bundesländer über Gesetze, die den Bürgern grundsätzlich den voraussetzungslosen Zugang zu den bei den Verwaltungen gespeicherten Informationen gewähren. Im Bund und bei weiteren Ländern ist die Einführung solcher Gesetze ebenfalls geplant.

Das Angebot eines Zugangs zu Informationen im Rahmen von eGovernment ist in vielen Fällen aber nicht allein auf diejenigen Bundesländer beschränkt, in denen bereits ein Informationsfreiheitsgesetz existiert. So gibt es in jeder Verwaltung eine Vielzahl von Informationen, die unabhängig von solchen Gesetzen ohne weiteres zur Verfügung gestellt werden können. Grenzen werden insofern vor allem durch den Schutz öffentlicher Belange, durch das Recht auf informationelle Selbstbestimmung Dritter,

durch zu beachtende Geschäfts- und Betriebsgeheimnisse sowie durch bestehende Verschwiegenheitspflichten gesetzt. Hierdurch wird für den Einzelfall eine praktische Konkordanz zwischen den zunächst divergierenden Zielen von Datenschutz einerseits und Informationsfreiheit andererseits erreicht.

Die Informationsfreiheit muss im Rahmen von eGovernment nicht grundsätzlich neu bewertet werden. Das Recht auf Informationszugang besteht unabhängig von der Form, in der die Informationen vorliegen und in der sie zur Verfügung gestellt werden können. Informationsfreiheit wird allerdings im Rahmen von eGovernment stark an praktischer Bedeutung gewinnen. Im Zeitalter elektronischer Datenverarbeitung nimmt die Menge an in elektronischer Form gespeicherten Informationen permanent zu. Es liegt also nahe, die elektronische Datenverarbeitung auch dafür einzusetzen, den Zugang zu diesen Informationen zu erleichtern. Elektronische Informationen lassen sich wesentlich leichter strukturieren, sie sind auf einfache Weise abrufbar, sie stehen schneller zur Verfügung und können wesentlich einfacher weiterverarbeitet werden, als dies bei einer konventionellen Verwaltung der Fall ist.

Als technologische Basis für einen elektronischen Informationszugang bietet sich nicht ausschließlich das Internet an. Informationsfreiheit als eGovernment-Lösung wäre z. B. auch unter Nutzung von Call Centern denkbar. Ebenso können den Bürgerinnen und Bürgern auch in ihrem gemeindlichen Bürgerbüro Informationen anderer öffentlicher Stellen z.B. unter Nutzung verwaltungsinterner Netze zugänglich gemacht werden. Aufgrund der zwischenzeitlichen Verbreitung, der Möglichkeit der visuellen Darstellung von Informationen und des bequemen Zugangs vom heimischen PC aus bietet sich der Zugang über das Internet aber in besonderer Weise an.

3.8 Standardisierung der Anwendungen und Werkzeuge

Für einen wirklich breiten Einsatz von eGovernment ist eine frühzeitige Vereinheitlichung und Standardisierung der Verfahrenslösungen und der dafür eingesetzten Werkzeuge unverzichtbar. Dazu gehört auch die Interoperabilität zwischen Systemen unterschiedlicher Hersteller und Dienstleister. Eine zu starke Aufsplitterung führt nicht nur zu unvertretbar hohen Entwicklungskosten bei den vielen unterschiedlichen staatlichen und kommunalen Trägern und zu unsinniger Doppelarbeit, sondern behindert vor allem einen wirklich breiten, auf Akzeptanz stoßenden Praxiseinsatz von eGovernment. Durch Bemühungen insbesondere des DIN und des KoopAADV sowie der Begleitforschung zu den Media@Komm-Projekten sind hier erste wichtige Schritte eingeleitet worden. Darüber hinaus erarbeitet die OSCI-Leitstelle für die öffentliche Verwaltung (www.osci.de) Standards in den Bereichen der sicheren Datenübermittlung sowie der Datenformate und Datenrepräsentation. Diese Aufgabenkonzentration an zentraler Stelle ist besonders zu begrüßen, da bei der Umstellung der Geschäftsprozesse auf den neuen Vertriebskanal Internet deutlich wird, dass die Vorgaben z.B. an rechtsverbindliche Zeitstempel und Quittungen nicht isoliert von der Frage der Datensicherheit betrachtet werden können. Auch die Ansätze des Bundes, die einzelnen eGovernment-Aktivitäten im Rahmen des IT-Zukunftskonzeptes und der Initiative BundOnline2005 in eine integrierte Gesamtarchitektur einzubinden und Basiskomponenten für die Bereiche Vorgangsbearbeitung, Datensicherheit, Content-

Management-System, secure eMail, Zahlungsverkehrsplattform und Formularserver entwickeln zu lassen, fördern die notwendige Vereinheitlichung.
Datenschutz und Datensicherheit sind für die Ausprägung der Standardisierungen ein wesentlicher Baustein. Sie sind mitentscheidender Vertrauensfaktor für eine breite Akzeptanz bei Bürgern, Wirtschaft und Verwaltung.

4 Herausforderungen für den Datenschutz

4.1 Generelle Bedrohungen

Unsichtbarkeit elektronischer Informationen

Elektronisch gespeicherte und übertragene Daten sind ohne technische Hilfsmittel nicht lesbar. Das kann dazu führen, dass selbst ordnungsgemäß gespeicherte Informationen ohne entsprechende Hard- und Software nur noch fehlerhaft oder gar nicht mehr interpretiert werden können, Nutzer nicht mehr in der Lage sind zu prüfen, ob Daten tatsächlich in der von ihnen gewollten Weise verarbeitet (gespeichert, verschlüsselt, gelöscht usw.) werden und dass Kopie und Original digitaler Dokumente nicht voneinander zu unterscheiden sind.

Flüchtigkeit elektronischer Informationen

Für elektronisch gespeicherte Informationen besteht prinzipiell die Gefahr des Verlustes, ohne dass irgendwelche Spuren verbleiben. Ursache können Entmagnetisierung von magnetischen Datenträgern durch Alterung, Temperatur, Luftfeuchte, äußere Magnetfelder, versehentliches oder vorsätzliches Löschen oder Überschreiben von Dateien und technisches Versagen von Festplatten sein.

Veränderung räumlicher Relation

Die ständig zunehmende Vernetzung ermöglicht den Zugriff auf elektronisch gespeicherte Daten unabhängig vom Ort (weltweit) und vom Endgerät (Großrechner, Personalcomputer, Handy, PDA usw.) des Abrufenden. Grenzüberschreitende Telekommunikationssysteme ermöglichen, dass nationalstaatliche Regelwerke sowohl von Informationsanbietern als auch von -nutzern umgangen werden.

Protokollierung/Revisionssicherheit

Die Verwaltung begibt sich in zunehmendem Maße in die Abhängigkeit von elektronischen Datenverarbeitungssystemen. Für die Revision der Datenverarbeitungsvorgänge sind Protokolle von entscheidender Bedeutung. Solange diese Protokolle jedoch nur in elektronischer Form vorliegen, unterliegen sie mit Blick auf die beschriebene Unsichtbarkeit und Flüchtigkeit elektronisch gespeicherter Informationen den gleichen Gefährdungen wie die verarbeiteten Daten selbst.

4.2 Spezifische Bedrohungen

Zunahme personenbeziehbarer Daten

Das öffentliche Kommunikationsnetz Internet offenbart systembedingt viele Informationen über seine Nutzer. Name und Adresse, die der Absender der eMail beistellt, Zeitpunkt, Dauer, Datenmenge und das verwendete Protokoll, den Standort des Endgeräts des Absenders oder Empfängers, das Netz, von dem die Nachricht ausgeht

oder an das gesendet wird, Beginn, Ende und Dauer einer Verbindung, all das sind personenbeziehbare Informationen, die viel über die handelnden Personen aussagen und die ausgewertet werden können. Die wichtigste Schaltstelle von eGovernment sind die Kommunikationsschnittstellen zwischen Verwaltung und Nutzern (virtuelle Poststelle, Behördenportal, Internet-Portal, Intermediär). Da an diesen Schnittstellen sämtliche Kommunikationsvorgänge zusammenlaufen, entstehen umfangreiche Datensammlungen und damit neuartige Bedrohungen für die Privatsphäre der Bürgerinnen und Bürger. Daraus erwachsen folgende Gefahren:

- Die gesamte Kommunikation Einzelner mit Behörden kann erfasst und analysiert werden,
- Daten können zusammengeführt und zu Persönlichkeitsprofilen verdichtet werden und
- die Zweckbindung elektronisch übertragener Daten kann durchbrochen werden.

Zentrale Datenbestände
Für eGovernment-Verfahren werden oft zentrale, bereichsübergreifende Datenbestände angelegt. Dies erscheint erforderlich, um Bürgern und Unternehmen Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer zentralen Stelle oder mit einem elektronischen Verfahren (One-Stop-Government, Lebenslagenkonzept) anbieten zu können. Daraus resultieren folgende Bedrohungen:

- Gefährdung der Zweckbindung gespeicherter Datenbestände,
- Gefährdung der „informationellen Gewaltenteilung“,
- mangelnde Transparenz für Betroffene (wer greift zu welchem Zweck auf welche Daten zu) und
- unzulässiges Aufspüren unbekannter Zusammenhänge mit Data Mining.

Automatisierung von Einzelentscheidungen
Die ständig zunehmende Menge und die relativ einfache Zusammenführung von elektronisch gespeicherten Informationen über einzelne Personen kann dazu führen, dass Entscheidungen ausschließlich aus der automatischen Bewertung einzelner gespeicherter Persönlichkeitsmerkmale resultieren. Für den Betroffenen kann das bedeuten, dass seine persönlichen Belange und Interessen nicht berücksichtigt werden, weil keine natürliche Person in den Entscheidungsprozess einbezogen wird oder er nicht in der Lage ist, persönliche Interessen geltend zu machen.

Fehlende Einbeziehung der Beschäftigten, Personalvertretungen oder Datenschutzbeauftragten
eGovernment-Projekte bringen nicht nur technische, sondern auch umfassende organisatorische Veränderungen in den beteiligten öffentlichen Stellen mit sich. Die Akzeptanz neuer Arbeitsabläufe, Tätigkeitsfelder und Datenschutzmaßnahmen durch Mitarbeiterinnen und Mitarbeiter dieser Behörden ist gefährdet, wenn die Beschäftigten nicht von Anfang gemeinsam mit den Personalvertretungen in die Planung von eGovernment-Projekten einbezogen, über Datenschutz- und Sicherheitsmaßnahmen nicht rechtzeitig und umfassend sensibilisiert und informiert oder Personalvertretun-

gen und Datenschutzbeauftragte nicht frühzeitig in die Planung von einzelnen Datenverarbeitungsvorgängen eingebunden werden.

4.3 Bedrohungen bei der Daten verarbeitenden Stelle

Manipulation der eigenen Infrastruktur
eGovernment-Anwendungen erfordern elektronische Kommunikation zwischen Bürgern und behördeninternen IT-Systemen. Die dafür erforderliche „Öffnung“ des Verwaltungssystems kann zu erheblichen Gefährdungen für die Integrität und die Vertraulichkeit der personenbezogenen Daten der Behörde führen. Schadprogramme wie Viren, Würmer oder Trojanische Pferde können die Rechner und andere Komponenten des Dienststellennetzes nachhaltig schädigen.

Manipulation des eGovernment-Angebots
Das eGovernment-Angebot wird in der Regel außerhalb des gesicherten Bereichs von Behördennetzen zum Abruf bereitgestellt. So kann beispielsweise der direkte Zugriff auf interne Datenbanken verhindert werden. Dadurch entsteht jedoch prinzipiell die Gefahr der Manipulation der angebotenen Informationen, weil die besonderen Schutzmechanismen außerhalb nicht wirken.

Bedrohung im Bereich der Anwendungen
Eine mangelhafte Benutzer- und Rechteverwaltung kann dazu führen, dass Unberechtigten Zugang zu personenbezogenen Daten gewährt wird. Derartige Gefährdungen entstehen, wenn beispielsweise eine gemeinsame Benutzerkennung von mehreren Bediensteten genutzt wird, Anwendungen durch Mitarbeiter ausgeführt werden, die die betreffenden Daten für ihre Aufgabenstellung nicht benötigen, oder Benutzer innerhalb eines spezifischen Verfahrens über Rechte verfügen, die sie für die Aufgabenerledigung nicht benötigen.

Angriffe auf sicherheitstechnische Einrichtungen
Sicherheitssysteme (Hard- und Software) unterliegen besonders schnellen technischen Veränderungen. Bedrohungen für die verantwortliche Stelle entstehen insbesondere, wenn Protokolle nicht regelmäßig ausgewertet werden, Software nicht regelmäßig aktualisiert wird, veraltete und damit unsichere Verschlüsselungs- oder Signaturverfahren eingesetzt werden oder mit Zertifikaten oder geheimen Schlüsseln nicht ordnungsgemäß umgegangen wird.

Unzulässiger Umgang mit elektronisch gespeicherten Daten
Gefährdungen für die Zweckbindung, Verfügbarkeit und Integrität ergeben sich, wenn Berechtigte nicht sorgsam mit personenbezogenen Daten umgehen. Beispiele hierfür sind:

- unzulässige Datenübermittlung (fahrlässig oder vorsätzlich) an Dritte,
- versehentliche Löschung oder Veränderung durch fehlende Sorgfalt bei der Verarbeitung,
- unzureichende Benutzer- und Rechteverwaltung,
- fehlende Zuständigkeitsregelungen für die Pflege zentraler Datenbestände,

- zu umfassender Online-Zugriff auf die automatisierten Datenbestände der Behörde (etwa durch einen Behördenleiter).

4.4 Bedrohungen beim Transport

Die Eigenschaften des Transportweges bei der elektronischen Übertragung personenbezogener Daten über öffentliche Netze sind dem Absender und dem Empfänger weder bekannt noch durch sie beeinflussbar. Das betrifft sowohl den Leitungsweg als auch die Anzahl und die Lokation der von den Daten passierten Vermittlungsrechner. Bei der Kommunikation über öffentliche Leitungen muss mit folgenden Gefährdungen gerechnet werden:

- Manipulation der Daten bei der Übertragung durch gezielte Angriffe oder technische Fehlfunktionen,
- Vortäuschen einer falschen Identität oder Verschleierung der Herkunft von Daten durch unzureichende Authentisierung,
- Übernahme von Verbindungen, wenn etwa Zeitstempel, kryptographisch erzeugte Prüfsummen oder elektronische Signaturen fehlen,
- Angriffe auf Protokolle und Dienste durch Manipulation des HTML-Codes oder infolge artfremder Nutzung des HTTP-Protokolls bzw. des HTTP-Ports 80.

4.5 Bedrohungen beim Nutzer von eGovernment-Anwendungen

Es ist nicht immer sichergestellt, dass beim Empfänger elektronisch übermittelter personenbezogener Daten ein ausreichendes Datenschutz- und IT-Sicherheitsniveau realisiert ist. Dadurch kann beispielsweise die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der übermittelten Daten, aber auch die Funktionsfähigkeit der technischen Infrastruktur des Empfängers gefährdet werden. Auch daraus resultieren Gefährdungen wie z.B. fehlerhafte Datenverarbeitung durch veraltete oder fehlerhafte Software (z. B. Viren, Trojanische Pferde, Aktive Inhalte, fehlerhafte Einstellungen, Programmfehler) oder fehlerhafter Hardware (z. B. falsch installiert, schlecht gewartet, nicht ausreichend geprüft), Analyse des Nutzerverhaltens durch unzulässige Auswertung von Protokolldaten (Zeitpunkt der Anmeldung, Zugriff auf Dokumente, Dauer der Verbindung usw.) und Gefährdungen für die Zweckbindung, wenn rechtmäßig übermittelte Daten vom Empfänger für andere Zwecke verwendet werden, als für die sie übermittelt wurden.

5 Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit

5.1 Gewichtung personenbezogener Daten

Personenbezogene Daten sind im Hinblick auf den Schutzbedarf sowohl einzeln als auch im Gesamtkontext der Anwendung zu bewerten. Wirken verschiedene Stellen an der eGovernment-Anwendung mit, ist darauf zu achten, dass die Daten der beteiligten Einrichtungen insgesamt bewertet werden. Die Ausgestaltung der Schutzmaßnahmen muss sich daran orientieren, welche Folgen für einen Betroffenen durch die Beeinträchtigung des informationellen Selbstbestimmungsrechts entstehen können und welcher potentielle Schaden für den Betreiber eintreten kann.

Anhaltspunkt für einen Schutzbedarf „niedrig bis mittel“ könnte z. B. sein, wenn
- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts durch den Einzelnen noch als geringfügig eingeschätzt würde;
- ein möglicher Missbrauch personenbezogener Daten nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen hätte;
- für den Betreiber der Anwendung nur eine geringe Ansehens- oder Vertrauensbeeinträchtigung zu erwarten wäre.

Anhaltspunkt für einen Schutzbedarf „hoch“ könnte z. B. sein, wenn
- eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen möglich erscheint;
- ein möglicher Missbrauch personenbezogener Daten erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen hätte;
- für den Betreiber der Anwendung eine breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten wäre.

Anhaltspunkt für einen Schutzbedarf „sehr hoch“ könnte z. B. sein, wenn
- eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen möglich erscheint;
- ein möglicher Missbrauch personenbezogener Daten für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten würde;
- für den Betreiber der Anwendung eine landes- bzw. bundesweite Ansehens- oder Vertrauensbeeinträchtigung denkbar ist.

Handlungsempfehlungen
- ☞ Als Hilfsmittel zur Orientierung können die Hinweise zur Schutzbedarfsfeststellung im entsprechenden Kapitel des IT-Grundschutzhandbuches (www.bsi.de/gshb/) angewendet werden.
- ☞ Die im Ergebnis notwendigen organisatorischen und technischen Maßnahmen zur Gewährleistung des informationellen Selbstbestimmungsrechts des Einzelnen sind konsequent umzusetzen; ist dies nicht oder nur teilweise möglich, muss unter Umständen auf die weitere Realisierung des Vorhabens verzichtet werden.

5.2 Erforderlichkeit und Verhältnismäßigkeit

Die Einhaltung des Erforderlichkeitsgrundsatzes im Einzelfall ist bereits in der Konzeptions- und Planungsphase von eGovernment-Anwendungen und bei der Systemauswahl zu berücksichtigen. Insofern korrespondiert die Vorgabe mit den Geboten zur Datenvermeidung und -minimierung (vgl. 5.3). Das Gebot der Erforderlichkeit gilt für alle Phasen der Verarbeitung, also nicht nur für die Erhebung, sondern auch für den gesamten anschließenden Verarbeitungsprozess. Daten, die für den weiteren Verwaltungsvollzug ab einer bestimmten Stufe nicht (mehr) erforderlich sind, sind zu löschen oder, wenn sie für bestimmte Kontroll- oder Nachweisfunktionen im Einzelfall noch benötigt werden, zu anonymisieren oder zumindest zu pseudonymisieren. Diese Maßnahmen können von modernen DV-Systemen dynamisch durchgeführt werden, d.h. bei Überschreiten eines bestimmten Termins (Löschfrist, Antragsende, Ablauf der

Wirkung eines Verwaltungsaktes) oder bei Eintritt eines bestimmten Ereignisses (der geforderte Nachweis wird erbracht) werden entsprechende Datenfelder gelöscht.

Handlungsempfehlungen

- ☞ Der Umfang der personenbezogenen Daten, die bei einer eGovernment-Anwendung erhoben, verarbeitet und genutzt werden sollen, ist in einer verbindlichen Regelung vorab festzulegen.
- ☞ Angebote, bei denen eine persönliche Identifikation des Bürgers bzw. der Bürgerin nicht erforderlich ist (z. B. Formularabruf), müssen ohne Erhebung der Identifikationsdaten genutzt werden können.
- ☞ Bei reinen Informationsangeboten sollte auf eine vollständige Erfassung der IP-Adressen der Nutzer verzichtet werden, da diese für die Erbringung des Angebots und seine Abrechnung nicht erforderlich sind. Für die statistische Auswertung reichen gekürzte IP-Adressen aus.
- ☞ Bei eMail-Newslettern reicht die Erhebung der eMail-Adresse der Empfänger aus; die Erfassung des Namens und der postalischen Anschrift kann unterbleiben.
- ☞ Bei eGovernment-Dienstleistungen dürfen nur diejenigen Nutzungsvorgänge protokolliert werden, bei denen dies aufgrund gesetzlicher Vorgaben erforderlich ist (z.B. automatisierte Abrufverfahren). Darüber hinaus dürfen Daten dann gespeichert werden, wenn konkrete Anhaltspunkte für eine missbräuchliche Inanspruchnahme vorliegen und soweit die Daten zur Missbrauchsaufklärung erforderlich sind. Diese Daten dürfen nicht für andere Zwecke genutzt werden.
- ☞ Elektronische Erhebungsformulare sind so zu gestalten, dass im Regelfall nur diejenigen Daten abgefragt werden, die für die jeweilige Aufgabe erforderlich sind. Sofern auch "Überschussdaten" erhoben werden, ist ausdrücklich auf die Freiwilligkeit der entsprechenden Angaben hinzuweisen. Bei der Übernahme analoger Formulare im Rahmen von eGovernment-Anwendungen ist vorab besonders kritisch zu prüfen, ob wirklich alle bisher erhobenen Daten für die Aufgabenerledigung der Verwaltung erforderlich sind.
- ☞ Da Dokumente bei bestimmten Formaten in der jeweiligen Textsoftware unsichtbare überarbeitete Teile und nicht notwendige personenbezogene Daten enthalten können und die Gefahr besteht, dass Formulare vor dem Ausdrucken und Versenden modifiziert werden können, sollten zum Download angebotene Formulare in einem datenschutzgerechten Format gestaltet und je nach Bedarf ganz oder teilweise gegen Modifikation gesichert sein.
- ☞ Wenn verschiedene Stellen bei der Erbringung einer eGovernment-Dienstleistung zusammenwirken, ist darauf zu achten, dass die beteiligten Einrichtungen nur die für die jeweilige Teilaufgabe erforderlichen Daten zur Kenntnis nehmen können.
- ☞ Definition und Dokumentation aller Daten verarbeitenden Systeme und Teilsysteme und Arbeitsschritte einschließlich ihrer Schnittstellen, in denen
  - ohne personenbezogene Daten gearbeitet werden kann,
  - personenbezogene Daten anonymisiert werden können,
  - personenbezogene Daten pseudonymisiert werden können bzw.
  - der direkt herstellbare Personenbezug unvermeidlich ist.

  Ist eine Anoymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System/Teilsystem oder den jeweiligen Arbeitsschritt eine entsprechende Prozedur zu finden, die die personenbezogenen Daten frühestmöglich anonymi-

siert bzw. pseudonymisiert (siehe hierzu auch Orientierungshilfe „Datenschutzfreundliche Technologien“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder).
- ☞ Systemtechnische Unterstützung der Reduzierung des Datenumfangs bei der Datenübermittlung (Batchverfahren).
- ☞ Setzen von logischen und termingesteuerten Lösch-/Speicherfristen.
- ☞ Laufende Überprüfung der elektronischen Formulare auf Aktualität und darauf, welche Datenfelder für welche Verwaltungsleistung benötigt werden.
- ☞ Gestaltung dynamischer Erhebungsbögen mit dynamischen Hinweisen, ob die Angabe freiwillig oder gesetzlich gefordert ist.
- ☞ Erneute Plausibilitätsprüfung bei der Übernahme der Daten aus dem elektronischen Formular in das DV-System.

5.3 Datenvermeidung und Datensparsamkeit

Das Gebot der Datenvermeidung und Datensparsamkeit verlangt von der verantwortlichen Stelle eine aktive Gestaltung ihrer technisch-organisatorischen Verfahren in der Form, dass möglichst keine oder so wenig personenbezogene Daten wie möglich verarbeitet werden. Über das Erforderlichkeitsprinzip hinaus fordert es von der verantwortlichen Stelle, die Umstände der Erforderlichkeit, die Zwecke und Prozesse der Datenverarbeitung zu überprüfen und mit dem Ziel der Vermeidung von Daten oder ihres Personenbezugs zu gestalten.

Handlungsempfehlungen
- ☞ Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass sie ohne personenbezogene Daten durchgeführt werden können.
- ☞ Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass die Verarbeitung personenbezogener Daten minimiert wird, indem weitgehend auf einen Personenbezug verzichtet wird.
- ☞ Insbesondere ist auf eine Identifizierung der Betroffenen zu verzichten, soweit dies nicht rechtlich gefordert wird.
- ☞ In den Fällen, in denen es nur auf eine Berechtigung (z.B. Gebühr bezahlt) oder eine bestimmte Eigenschaft (z.B. Arzt) ankommt, ist nur deren Vorliegen zu prüfen und auf die Identifizierung des Handelnden zu verzichten.
- ☞ Soweit technisch möglich und zumutbar, ist den Betroffenen zu ermöglichen, anonym oder pseudonym zu handeln.
- ☞ Soweit technisch möglich und zumutbar, ist den Betroffenen zu ermöglichen, anonym oder pseudonym zu bezahlen. Hierfür können unterschiedliche Zahlungsverfahren genutzt werden, die diese Möglichkeit bieten (s. Kapitel 5.7.6)

5.4 Einwilligung in die Datenverarbeitung und die Nutzung des elektronischen Weges, elektronische Einwilligung

Bei fehlender einschlägiger Rechtsvorschrift darf die Datenverarbeitung nur mit vorheriger Zustimmung des Betroffenen erfolgen (Einwilligung). Die Einwilligung bei e-Government-Anwendungen kann auch elektronisch erklärt werden. Sind die gesetzli-

chen Voraussetzungen für eine beabsichtigte Datenverarbeitung, insbesondere im Zusammenhang mit Maßnahmen der Hoheitsverwaltung, nicht erfüllt, kann die fehlende gesetzliche Befugnis grundsätzlich aber nicht durch eine Einwilligung des Betroffenen ersetzt werden.

Handlungsempfehlungen

- ☞ Die verantwortliche Stelle hat die Betroffenen im Vorfeld der Erklärung hinreichend über
  - Umfang, Form und Zweck der Datenverarbeitung,
  - mögliche Verknüpfungen mit anderen Datenbeständen und potenzielle Empfänger der Daten, insbesondere wenn diese ihren Sitz in einem Staat außerhalb der Europäischen Union haben,
  - die Freiwilligkeit der Einwilligung, die Möglichkeit einer Verweigerung und deren Folgen,
  - die Widerruflichkeit der Einwilligung

  zu unterrichten.
- ☞ Soweit die Zustimmung auf einem Formular erfolgt, sind die Anforderungen an die Bestimmtheit des Hinweises und der Einwilligung identisch.
- ☞ Die beantragte Entscheidung einer Behörde darf nicht von der Einwilligung abhängig gemacht werden. Auch bei rechtlicher oder faktischer Abhängigkeit (z.B. im Verhältnis Arbeitnehmer – Arbeitgeber) ist die Entscheidungsmöglichkeit der Betroffenen wesentlich eingeschränkt und die Freiwilligkeit gefährdet.
- ☞ Sollen besonders schützenswerte Daten im Sinne des § 3 Abs. 9 BDSG verarbeitet werden, muss sich die schriftliche Einwilligung ausdrücklich auch auf diese Daten beziehen. Die Erklärung der Einwilligung sollte zum Schutz des Betroffenen und aus Gründen der Nachvollziehbarkeit grundsätzlich schriftlich erfolgen.
- ☞ Bei der Einwilligung handelt es sich um eine höchstpersönliche Erklärung, für die Geschäftsfähigkeit nicht vorausgesetzt wird. Bei Minderjährigen ist aber auf die notwendige Einsichtsfähigkeit nach dem jeweiligen Reifezustand zu achten.
- ☞ Um ihre Warnfunktion zu erfüllen, darf die Einwilligung nicht beiläufig abverlangt werden. Bloße Hinweise auf die allgemeinen Geschäftsbedingungen sind nicht ausreichend. Auch Merkblätter und andere Informationsmaterialien, in denen die Verarbeitung der Daten ausführlich erläutert wird, erfüllen nicht die gesetzlichen Anforderungen. Soll die Einwilligung im Zusammenhang mit anderen Erklärungen erteilt werden, ist sie im Schriftbild (Fett- oder Kursivdruck, Einrahmung) hervorzuheben.

<u>Einwilligung zur Nutzung des elektronischen Weges:</u>

- ☞ Die Verwaltung sollte für die Nutzung des elektronischen Weges die Zustimmung des Betroffenen einholen, um spätere Unsicherheiten auszuschließen. Zuvor sind die Betroffenen ausführlich über die Rechtsfolgen (z.B. die Pflicht zur Aufrechterhaltung der elektronischen Adresse, die regelmäßige zeitnahe „Leerung“ ihres elektronischen Postfaches und ggf. die Anforderungen an Signaturen) zu informieren. Aus der bloßen Bekanntgabe einer eMail-Adresse sollte ein Einverständnis zur Entgegennahme elektronischer Dokumente der Verwaltung nicht abgeleitet werden.

Elektronische Einwilligung:

- ☞ Eine elektronisch erklärte Einwilligung ist grundsätzlich nur wirksam, wenn das Dokument mit einer qualifizierten elektronischen Signatur versehen ist. Für die Datenverarbeitung in Tele- und Mediendiensten ist eine vereinfachte Form der elektronischen Einwilligung vorgesehen. Für die Aufnahme einer Adresse in einen Informationsverteiler genügen danach z.B. die folgenden Voraussetzungen:
  - Es muss eine eindeutige und bewusste Handlung des Nutzers (opt-in-Lösung) erfolgen.
  - Mit Hilfe der Protokollierung muss festgehalten werden, dass der Nutzer seine Einwilligung gegeben hat.
  - Die jederzeitige Abrufbarkeit der Einwilligung muss gewährleistet sein.
  - Der Nutzer ist vor der Erklärung der Einwilligung auf sein Widerspruchsrecht hinzuweisen.

5.5 Sicherung der Zweckbindung

Da bei eGovernment-Anwendungen verknüpfbare Sammlungen von personenbezogenen Daten entstehen, muss besonders darauf geachtet werden, dass diese Daten wirklich nur für die Zwecke verwendet werden, für die sie erhoben und gespeichert wurden. Nur in für den Bürger klar überschaubaren Grenzen, nämlich aufgrund einer ausdrücklichen gesetzlichen Erlaubnis oder mit Einwilligung des Betroffenen, dürfen diese Daten auch für andere Zwecke verwendet werden. Die Zweckbindung muss vorsorglich durch organisatorische und technische Maßnahmen gesichert werden.

Handlungsempfehlungen

- ☞ Es muss sichergestellt sein, dass nur berechtigte Nutzer den Zugang zu den Daten haben. Die Identifizierung und Authentisierung sollte an zentraler Stelle durchgeführt werden (Authentifizierungsserver) bzw. über das jeweilige Betriebssystem erfolgen.
- ☞ Rechte sind sowohl benutzerbezogen als auch datei- oder programmbezogen zu vergeben, um die Zugriffsmöglichkeiten zweckgebunden zu begrenzen. Dabei ist der Maßstab immer das fachliche Anforderungsprofil und die Arbeitsaufgabe des einzelnen Benutzers.
- ☞ Arbeitsschritte, die im Hinblick auf die Einhaltung der Zweckbindung besonders sensibel sind, sind zu Zwecken der Beweissicherung soweit notwendig zu protokollieren. Beweissicherung bedeutet in diesem Zusammenhang, dass es im Nachhinein möglich sein muss, den Missbrauch zugestandener Rechte nachzuweisen oder die versuchte Ausübung von nicht zugestandenen Rechten aufzudecken.
- ☞ Daten sind logisch getrennt zu speichern. In diesem Fall ist eine gegenseitige Abschottung der zweckgebundenen Datenbestände am einfachsten und am datenschutzfreundlichsten zu realisieren.
- ☞ Moderne Datenverarbeitungsanlagen bieten die Möglichkeit, gleichzeitig mehrere Anwendungen abzuarbeiten. Hier ist darauf zu achten, dass die einzelnen Anwendungen und ihre jeweils zweckgebundenen Daten gegenseitig voneinander abgeschottet verarbeitet werden. Dies kann in der Praxis durch den Einsatz technischer Zusatzsysteme erreicht werden, die beispielsweise auf einem Prozessor

mehrere virtuelle Maschinen simulieren, welche die jeweiligen Anwendungen einschließlich deren Daten gegeneinander abgekapselt verarbeiten.

- ☞ Sensible Daten sind verschlüsselt zu speichern und zu übertragen, damit eine inhaltliche Kenntnisnahme der Daten durch Unbefugte verwehrt wird. Die Prozeduren der Verschlüsselung sind für die Benutzer transparent zu halten.
- ☞ Für besondere Zwecke erhobene Daten sollten mit einem spezifischen Kennzeichen versehen werden, welches den Zweck ihrer Erhebung sowie einer eventuellen Verarbeitung und Übermittlung spezifiziert, sodass eine Verwendung für einen anderen Zweck kontrolliert werden kann. Die Vergabe solcher Kennzeichen und die Sicherung der Zweckbindung anhand der Auswertung dieser Kennzeichen, stellt eine elegante und zukunftsorientierte Sicherheitstechnologie dar. Für ihre technische Realisierung wären allerdings erhebliche Änderungen bzw. Erweiterungen der bestehenden Betriebs- und Datenbanksysteme sowie Anwendungsprogramme erforderlich, die derzeit noch nicht über solche Funktionalitäten verfügen.

5.6 Transparenz

Nur wenn die Bürgerinnen und Bürger wissen, wie die Datenverarbeitungsvorgänge ablaufen, haben sie auch die Möglichkeit, ihre Rechte wahrzunehmen. Für viele Nutzer wird allerdings nicht ohne weiteres erkennbar sein, an welchen Stellen sie bei Nutzung elektronisch zur Verfügung gestellter Informationen Spuren hinterlassen bzw. inwieweit personenbezogene Nutzerdaten weiterverarbeitet werden. Das Teledienstedatenschutzgesetz und der Mediendienstestaatsvertrag verpflichten die Diensteanbieter für den Fall der automatisierten Weiterverarbeitung personenbezogener Daten, die Nutzer zu Beginn des Verfahrens zu unterrichten. Nur die Vorabinformation versetzt die Nutzer in die Lage darüber zu entscheiden, ob sie das Nutzungsverhältnis fortsetzen oder abbrechen möchten.

Handlungsempfehlungen:

- ☞ Die Datenschutzhinweise sollten eine Erklärung enthalten zu Grundsätzen der Verfahrensweise bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Angebots im Internet anfallen. Außerdem sollte über die Auskunftsansprüche und Korrekturrechte informiert werden. Die Hinweise sollten an zentraler Stelle – etwa auf der Eingangsseite im Internet - erscheinen und sollten leicht verständlich formuliert sein. Zur Gewährleistung der Transparenz gehört insbesondere die Information darüber, wer für die Gestaltung des Angebots verantwortlich zeichnet.

Öffentliche Stelle: <Name>
Verantwortlich: <Name> <Adresse>
Telefon: <Nr.>
Telefax: <Nr.>
eMail: <eMail Adresse>
(Aus den Informationsgeboten des § 6 TDG bzw. § 6 MDStV ergebenen ggf. weitere Hinweispflichten.)

- ☞ Bei Links und eMail-Adressen sollte ein Hinweis auf die Risiken bzw. den Haftungsausschluss aufgenommen werden. Dies kann auch durch eine allgemeine Information in der Datenschutzhinweisen erfolgen. Es ist auch möglich, beim „Überstreichen“ eines Links oder einer eMail-Adresse den Hinweis automatisch aufzublenden.
- ☞ Bei Koppelung des Verwaltungsauftritts mit privaten Sponsoren muss für die Nutzer deutlich erkennbar sein, wer für welches Angebot die Verantwortung trägt.
- ☞ Wenn die Nutzung eines Angebots die Erhebung personenbezogener Daten voraussetzt, sind die Nutzer über die Zweckbestimmung der Verarbeitung, für die die Daten bestimmt sind, zu unterrichten. Wenn Daten in Log-Dateien gespeichert werden, könnte eine Information folgendermaßen aussehen:

> Mit Ihrem Zugriff auf diese Seite werden die um die letzten 3 Ziffern verkürzte IP-Adresse Ihres Rechners 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 der 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, wenden Sie sich bitte an:
> **Name: eMail-Adresse. Telefon:**

- ☞ Sollten Cookies verwendet werden, so muss die Information auch einen Hinweis über deren Auswirkungen enthalten. Mit der Verwendung aktiver Elemente wie Active-X, Java, JavaScript (siehe auch Kapitel „Sicherer Internet-Auftritt im eGovernment“ im eGovernment-Handbuch des BSI – www.bsi.egovernment-handbuch.de) sollten öffentliche Verwaltungen restriktiv umgehen. Die wesentlichen Informationen und Serviceleistungen sollte jeder Bürger ohne Eingehen der mit diesen Elementen verbundenen Risiken nutzen können. Sollte jedoch eine Verwaltung trotzdem nicht völlig auf die Nutzung dieser Elemente verzichten wollen, so hat sie den Nutzer auch hierüber zu informieren und ihn auf die Risiken hinzuweisen.
- ☞ Bei elektronischer Antragsstellung ist der Antragsteller darüber zu informieren, wie das Gesamtverfahren abgewickelt wird.
- ☞ Sollten im Rahmen von eGovernment-Anwendungen mobile Speichermedien zum Einsatz kommen, so muss für den Betroffenen erkennbar sein, welche Daten und Programme mit welchen Funktionen auf seiner Karte gespeichert sind. Insbesondere muss er erkennen können, wer welche Daten und Programme mit welchen Funktionen auf seiner Karte speichert (Schreibberechtigung) und wer welche Daten nutzen kann (Leseberechtigung). Zudem muss die Möglichkeit gegeben sein, den Inhalt der gespeicherten Informationen zur Kenntnis zu nehmen. Ferner ist er darüber zu unterrichten, welche Maßnahmen bei Verlust oder Zerstörung des Mediums zu treffen sind und welche Verfahren bei der verantwortlichen Stelle im Hintergrund ablaufen.

☞ Um für die Nutzer ein hohes Maß an Transparenz zu gewährleisten, sollten die Datenschutzerklärungen bei eGovernment-Anwendungen den P3P-Standard (www.w3c.com/p3p) einhalten (siehe Kapitel 6.3).

5.7 Weitere anwendungsorientierte Handlungsempfehlungen

5.7.1 Elektronischer Behördenwegweiser/Informationsangebote

Bei der Kontaktaufnahme mit der Verwaltung ist den einzelnen Bürgerinnen und Bürgern häufig zunächst nicht bekannt, welche Stelle für ihr Anliegen zuständig ist. Während sie sich in herkömmlichen Verfahren zum zuständigen Sachbearbeiter "durchfragen", können sie beim eGovernment durch elektronische Auskunftssysteme die zuständige Stelle herausfinden und dabei auch Kontaktdaten (Telefonnummer, eMail-Adresse, Anschrift, Öffnungszeiten) und weitere Informationen über die Voraussetzungen einer bestimmten Leistung (z.B. Mitbringen von Passbildern, Vollmachten, Gebühren usw.) erhalten.

Handungsempfehlungen

☞ Elektronische Behördenwegweiser müssen so gestaltet werden, dass die Bürgerinnen und Bürger grundsätzlich ohne Nennung ihres Namens die erforderlichen Informationen erhalten.
☞ Eine personenbezogene Protokollierung der Abfragen hat zu unterbleiben.
☞ Soweit im Einzelfall zusätzliche Daten erforderlich sind, um die erwünschte Auskunft zu erteilen (z. B. Anschrift, Anfangsbuchstaben des Namens) muss sich die Erhebung auf die erforderlichen Angaben beschränken; eine Speicherung dieser Daten darf nicht stattfinden.
☞ Eine Veröffentlichung von Bedienstetendaten im Internet sollte nur erfolgen, wenn der Dienstverkehr es erfordert oder mit Einwilligung des Bediensteten. Dabei sind die besonderen Gefahren (z.B. Suchmaschinen), die mit einer Veröffentlichung im Internet verbunden sind, in die Abwägung einzubeziehen.
☞ Die Veröffentlichung von Bürgerdaten im Internet setzt in jedem Fall eine Einwilligung voraus.

5.7.2 eMail

Zahlreiche eGovernment-Lösungen beinhalten auch die Möglichkeit zum Austausch von eMails. Mit einer eMail können neben der Übermittlung des eigentlichen Inhalts auch Dateien als Attachement verbunden werden, die in digitaler Form längere Texte, Bilder, Töne, Filme, Programme etc. enthalten können. Das der elektronischen Post zugehörige Protokoll gewährleistet hierbei den Ablauf der Kommunikation. Die zu übermittelnden Daten werden mit einem Kopf versehen, der den Absender, Empfänger und weitere Informationen (Zeitpunkt des Absendens, den Weg der Nachricht und die verwendete Software) enthält, und verschickt. Im Internet gilt die Zustellung als erfolgt, wenn der Absender keine Rückmeldung über einen Zustellfehler erhält. Wichtigste Voraussetzung für das eMail-System ist, dass Sender und Empfänger jeweils eine eindeutige eMail-Adresse besitzen, die ähnlich der postalischen Anschrift funktioniert. Da die eMails auf verschiedenen Servern zwischengespeichert werden, ist es leicht möglich, dass eMails auch von unbefugten Personen gelesen, gefälscht, gelöscht oder mit Viren und Trojanischen Pferden (ausführbare Programmcodes) verse-

hen werden. Deshalb ist ein vorsichtiger Umgang damit erforderlich. Entsprechende Hinweise sind an die Beschäftigten und Nutzer/innen zu erteilen.

Gegenüberstellung der Risiken und Schutzmöglichkeiten:

Risiken	**Schutzmöglichkeiten**
Mitlesen durch Unbefugte	Verschlüsselung
Veränderung oder Verfälschung von Inhalt und Absender	elektronische Signatur
Löschen oder Verlust	Quittungsverfahren mit Empfänger vereinbaren
Viren und Trojanische Pferde	Anti-Virenprogramme

Handlungsempfehlungen:

☞ Wenn mit der eMail personenbezogene oder andere schutzbedürftige Daten übermittelt werden, sind diese Daten zu verschlüsseln. Daneben kann es auch notwendig sein, die Authentizität des Absenders nachzuweisen, etwa mit Hilfe einer elektronischen Signatur. Dafür bieten sich unterschiedliche Realisierungsmöglichkeiten:

- eMails mit einem gängigen eMail-Programm mit Hilfe des Internet-Mail-Protokolls SMTP versenden und dabei den Mail-Inhalt sowie die Anlagen mit einem speziellen Verschlüsselungsprogramm wie z. B. PGP verschlüsseln.
- Browserbasierte Verschlüsselung: Dabei werden die erfassten Daten SSL-verschlüsselt an einen von der öffentlichen Stelle dafür vorgesehenen Web-Server übertragen. Die Antwort der öffentlichen Stelle wird so bereitgestellt, dass der Bürger auch darauf SSL-geschützt zugreifen kann. Um unberechtigte Zugriffe auf die Antworten zu verhindern, ist eine Authentifizierung der Bürger erforderlich.
- Ist die Kommunikationsmöglichkeit auf Dauer eingerichtet, so bietet es sich an, die Bürger, die diesen Dienst nutzen wollen, vor der ersten Nutzung zu registrieren. Die öffentliche Stelle richtet dabei nach Überprüfung der Identität des Kunden für ihn ein persönliches eMail-Postfach auf dem Web-Server ein, in das alle Antwortschreiben an den Bürger abgelegt werden. Über eine Web-Schnittstelle kann der Bürger jederzeit hierauf zugreifen.
- Sind die zugrunde liegenden Kommunikationsvorgänge jedoch so gestaltet, dass in der Regel nur eine Antwort auf einen Bürgerantrag erfolgt, z. B. bei einer einfachen Melderegisterauskunft, so kann das Verfahren so gestaltet werden, dass der Bürger beim Stellen seines verschlüsselt übertragenen Antrags ein persönliches Passwort angibt, das er eingeben muss, bevor er auf die Antwort der Behörde zugreifen kann.

Im Hinblick auf die Gestaltung sicherer Kommunikation ist zu bedenken, dass die SSL-Verschlüsselung im Bereich der öffentlichen Stelle an dem von ihr genutzten Web-Server endet. Es kann sich daneben also ein zusätzlicher Schutzbedarf im Bereich des Web-Server-Betriebs ergeben, insbesondere wenn dieser nicht von der öffentlichen Stelle selbst erfolgt. Ferner gilt es, auch die Kommunikationswege zwi-

schen den Sachbearbeitern der eMails innerhalb der öffentlichen Stelle und dem Web-Server in die Sicherheitsüberlegungen mit einzubeziehen.

5.7.3 Virtuelle Poststelle der Behörde

Bei der Abwicklung der elektronischen Bürgerkontakte über eine zentrale Stelle in der Behörde (z.B. eGovernment-Portal) stellt sich die Frage, wie die Zuordnung zu den einzelnen Organisationseinheiten erfolgen kann. Grundsätzlich soll die Virtuelle Poststelle keine Kenntnis der Inhalte der Kommunikation erhalten. Daher erfolgt eine Adressierung über Zertifikatsinhalte oder andere Metainformationen über die Dokumente, die eine Weiterleitung ohne Zeitverzögerung an die zuständige Stelle (z.B. Sozialamt, Meldeamt) ermöglichen. Die Virtuelle Poststelle als Basiskomponente ‚Datensicherheit' fungiert als zentrales eMail-Gateway und Dienstleister für Web-Applikationen zur Sicherstellung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation zwischen Bürgern und Behörden.

Handlungsempfehlungen:

- ☞ Die Virtuelle Poststelle erhält keine Kenntnis von den Inhalten der Kommunikation (siehe hierzu auch Abschnitt 6.1.2). Dies kann bspw. durch „elektronische Briefumschläge" für die Inhaltsdaten, wie etwa nach dem OSCI-Standard, sichergestellt werden. Die Zuordnung zur fachlich zuständigen Stelle erfolgt über Zertifikatsdaten (Signatur-, Verschlüsselungs- oder Authentisierungszertifikat) bzw. andere Metainformationen, die den eigentlichen Inhaltsdaten beigefügt sind.
- ☞ Es dürfen jeweils nur die erforderlichen Daten an das Back-End weitergegeben werden.
- ☞ Die Inhaltsdaten müssen sowohl im Post-Eingangsbereich als auch bei der Weiterleitung an die fachlich zuständige Stelle gegen unberechtigte Zugriffe geschützt werden. Mit der Virtuellen Poststelle wird sicher gestellt, dass eine automatisierte Weiterleitung der Bürgerkontakte an die fachlich zuständige Stelle ohne inhaltliche Auswertung durch die übergreifende "Poststelle" erfolgt.
- ☞ Die Zuordnung der jeweiligen Vorgänge zu einer elektronischen Akte sollte nicht durch die virtuelle Poststelle, sondern durch die fachlich zuständige Stelle erfolgen. Nur sie kann letztlich die Relevanz der entsprechenden Informationen beurteilen und ihre genaue fachliche Zuordnung vornehmen.
- ☞ Zwischen jeder Fachstelle und einem zentralen Portal ist ein eigenes Auftragsverhältnis zu begründen und durch schriftliche Festlegungen abzusichern.

5.7.4 Notwendige und mögliche Identifizierung

Anonymes Surfen im Internet ist nicht nur zulässig, sondern rechtlich geboten. Die Vorschriften des TDDSG sowie des MDStV verpflichten den Diensteanbieter, dem Nutzer eine anonyme Inanspruchnahme seines Angebotes oder eine solche unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Mit dieser Verpflichtung hat der Gesetzgeber die allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit für die Diensteanbieter konkret geregelt. Andererseits werden im eGovernment an die sichere Identifizierung der Kommunikationspartner hohe rechtliche Anforderungen gestellt. Vor diesem Hintergrund werden elektronische Signaturen zu notwendigen Werkzeugen. Dabei ist zu beachten, dass die Signatur als

Unterschriftenersatz konzipiert und auch geregelt wurde. Insofern bildet das Zertifikat zwangsweise nur die Informationen ab, die auch mit einer eigenhändigen Unterschrift gegeben werden, nämlich Name und Vorname. Kein Bestandteil ist dabei die Adresse des Signaturschlüsselinhabers. Der Name und Vorname ermöglichen schon wegen der häufigen Namensgleichheiten keine eindeutige Identifizierung. Dies bringt erhebliche Probleme im gewohnten Identifizierungsverfahren einer Behörde, wo für manche Fachverfahren der Personalausweis als zusätzliche Identifizierung erforderlich ist.
Um personenbezogene Datenspuren im Identifizierungsverfahren zu vermeiden, sollte dem Signaturschlüsselinhaber die Möglichkeit gegeben werden, in einem qualifizierten Zertifikat anstatt seines Namens ein Pseudonym aufzuführen.

Handlungsempfehlungen:

- ☞ Die Verfahren sollten so gestaltet werden, dass eine anonyme Inanspruchnahme des Angebotes oder eine solche unter Pseudonym ermöglicht wird (Grundsatz der Datenvermeidung und Datensparsamkeit).
- ☞ Soweit eine Identifizierung zwingend geboten ist, dürfen die Anforderungen an die Identifizierung beim eGovernment jedenfalls nicht höher angesetzt werden als in dem Papierverfahren.
- ☞ Einsatz von Signaturen einschließlich der freiwilligen Erweiterung des Zertifikats um Anschrift und Geburtsdatum.
- ☞ Nutzung elektronischer Ausweise. Der Ausweis wäre eine von der Behörde signierte Datei, die der Signaturschlüsselinhaber jederzeit zu seiner eindeutigen Identifizierung selbstbestimmt in seine aktuell signierte Willenserklärung „einbinden“ kann. Dieses Verfahren ist erheblich datenschutzfreundlicher als die Erweiterung der Zwangsdaten eines Zertifikats oder die zwangsweise Speicherung der Identifikationsdaten in einem zentralen Verzeichnis.
- ☞ Einsatz von pseudonymen Signaturen. Für die Verwendung muss zwischen Trägern öffentlicher Ämter und Privatpersonen unterschieden werden. Im Regelfall dürfen die Träger öffentlicher Ämter hoheitliche Handlungen immer nur mit ihrem wahren Namen durchführen. Dagegen sollten Privatpersonen auch gegenüber der Verwaltung pseudonym handeln können, sofern nicht ihre Identifizierung zur Erfüllung der Verwaltungsaufgaben unabdingbar erforderlich ist.
- ☞ Wenn keine anderen Möglichkeiten zur Verfügung stehen und eine eindeutige Identifizierung des Handelnden durch die Behörde erforderlich ist, kann ein Identifizierungskataster gewählt werden.

Siehe hierzu auch Kapitel 6.3

5.7.5 Grunddaten im virtuellen Schließfach

Die häufigere Nutzung elektronischer Bürgerdienste kann dazu führen, dass jemand seinen Namen, seine Anschrift sowie weitere in anderen Zusammenhängen relevante Grunddaten immer wieder neu in die entsprechenden Eingabemasken eintragen muss. Um den Bürgerinnen und Bürger diese immer wiederkehrende Erfassung abzunehmen, kann ihnen die Möglichkeit geboten werden, dass Daten, die einmal erfasst worden sind, automatisch für die Bürgerdienste übernommen werden. Technisch können diese Daten auf einer Chipkarte des Bürgers gespeichert, auf dessen PC oder in einem besonderen Bereich des Internetportals hinterlegt werden. Eine

dezentrale Lösung ist unter dem Gesichtspunkt, das Entstehen zentraler Datensammlungen möglichst zu vermeiden, vorzuziehen.

Handlungsempfehlungen:

- ☞ Niemand kann dazu gezwungen werden, Daten auf Vorrat für Bürgerdienste zu hinterlegen.
- ☞ Die Erfassung, Änderung oder Löschung dieser Daten darf nur nach einer zuverlässigen Authentifizierung des Bürgers möglich sein. Die übertragenen Daten sind durch Verschlüsselung vor unberechtigter Kenntnisnahme und Verfälschung zu schützen.
- ☞ Es sollte stets die Möglichkeit geboten werden, die für die Nutzung eines konkreten Bürgerdienstes erforderlichen Daten erst im jeweiligen Einzelfall einzugeben.
- ☞ Der Bürger sollte frei darüber entscheiden können, welche Datenarten er für künftige Nutzungen hinterlegt.
- ☞ Die Speicherung sollte so erfolgen, dass nur die Bürger selbst auf die von ihnen hinterlegten Daten zugreifen und deren Transfer in einzelne Bürgerdienste veranlassen können.
- ☞ Der Bürger sollte die von ihm hinterlegten Daten jederzeit einzeln oder insgesamt löschen können. Um Datenfriedhöfe zu vermeiden, sollten hinterlegte Daten, die über eine längere Zeit hinweg nicht mehr genutzt wurden, automatisch gelöscht werden. Soweit der betreffende Bürger eine eMail-Adresse hinterlegt hat, kann er rechtzeitig vor der automatischen Löschung darüber informiert und ihm die Möglichkeit gegeben werden, die Löschung zu verhindern.
- ☞ Sofern die Daten in Chipkarten oder auf dem PC der Anwender hinterlegt werden sollen, sollten die Dienststellen, die von diesen Daten Gebrauch machen wollen, ein Sicherheitskonzept erarbeiten, das auch berücksichtigt, wie die in der Sphäre der Bürger gespeicherten Daten vor unberechtigten Zugriffen sowie vor Manipulation geschützt werden können.

5.7.6 Zahlungsverfahren

Um das gesamte Verwaltungsverfahren medienbruchfrei abzuwickeln zu können, muss auch der Zahlungsvorgang elektronisch realisiert werden.

Handlungsempfehlungen:

- ☞ Maßgebliches Kriterium für die Datenschutzfreundlichkeit ist die Datensparsamkeit der Verfahren. Wenn im Verwaltungshandeln eine Identifizierung nicht erforderlich ist, sollte auch die Zahlung grundsätzlich anonym oder pseudonym möglich sein. Dabei ist zu unterscheiden zwischen Anonymität bzw. Pseudonymität gegenüber der Verwaltung als Anbieter von Dienstleistungen, gegenüber beteiligten Banken oder Kreditinstituten und eventuell gegenüber einem als Treuhänder (Inkasso) agierenden, zwischengeschalteten Unternehmen. Anonymität bzw. Pseudonomität muss selbst dann gewahrt bleiben, wenn ein Nutzer zwei oder mehrere Male auf einen Dienst zugegriffen hat (Unverkettbarkeit).
- ☞ Sofern die Identifizierung des Nutzers nicht erforderlich ist, muss die Zahlung anonym oder pseudonym ermöglicht werden, soweit dies technisch möglich und zumutbar ist.

- ☞ Vertraulichkeit und Integrität der Daten sowie Authentizität aller am Zahlvorgang beteiligten Stellen müssen gewährleistet sein.
- ☞ Darüber hinaus ist ein hohes Maß an Transparenz erforderlich, damit Zahlungen nachvollziehbar sind, jederzeit Informationen über Guthaben bzw. Debit verfügbar sind und das Sicherheitsniveau auch für die Nutzer bewertbar ist.
- ☞ Für die Akzeptanz von Zahlungssystemen ist nicht zuletzt die Einfachheit der Bedienung und die Geschwindigkeit des Zahlvorgangs maßgeblich.

Beispiele für Zahlungssysteme

Aus datenschutzrechtlicher Sicht sind insbesondere solche Systeme empfehlenswert, die auf Guthabenbasis arbeiten. Sie ermöglichen prinzipiell anonyme und pseudonyme Zahlverfahren. Mit der vom Zentralen Kreditausschuss der Banken und Sparkassen (ZKA) herausgegebenen GeldKarte, der prepaid-Karte, MicroMoney der Telekom-Tochter DeTeCardService (http://www.detecardservice.de/de/micromoney/index.html) oder der aus Österreich stammenden paysafecard (http://www.paysafecard.com/de/de/index.html) stehen derartige Guthabenkarten am Markt zur Verfügung. Völlig anonym und deshalb besonders datenschutzfreundlich sind solche Kartensysteme, bei denen die Werteinheiten ausschließlich lokal auf der Chipkarte gespeichert sind und keine Schattenkonten geführt werden.

Nach wie vor sehr verbreitet sind Zahlungsvorgänge im Internet, bei denen dem Anbieter die Kreditkartennummer übermittelt wird. Für eGovernment-Anwendungen ist diese Zahlungsweise aber selbst dann nicht empfehlenswert, wenn die Übertragung der Kreditkartennummer etwa per SSL verschlüsselt erfolgt, da beispielsweise weder Anonymität des Karteninhabers noch die Sicherheit der Kredikartendaten gewährleistet ist. Die Nutzung der Kreditkarte als Zahlungsmittel kann jedoch erwogen werden, wenn Verfahren eingesetzt werden, die auf dem von VISA und Mastercard entwickelten Protokoll Secure Electronic Transaction (SET) basieren (http://www.goset.de). Sowohl Datensparsamkeit als auch Pseudonymität des Nutzers – insbesondere gegenüber dem eGovernment-Anbieter – werden hier weitgehend gewährleistet. Erwähnenswert ist in diesem Zusammenhang das Forschungsprojekt DASIT (Datenschutz in Telediensten; http://www.dasit.myshop.de). DASIT kann beispielsweise SET als pseudonymes Bezahlverfahren nutzen, sodass ein Online-Händler – und somit auch eine Behörde als Anbieter elektronischer Dienstleistungen – die Anforderungen des TDDSG und des BDSG an pseudonymes Einkaufen und Bezahlen im Internet erfüllen kann.

Einen anderen Ansatz verfolgen Zahlungssysteme, bei denen eine im Internet bestellte Dienstleistung unter Nutzung des Mobiltelefons bezahlt wird. Bestell- und Zahlungsvorgang nutzen mit Internet und GSM-Netz unterschiedliche Medien. Datenschutzrechtlich positiv zu bewerten ist, dass der Nutzer gegenüber dem Anbieter anonym bleibt und die sensiblen Daten des Zahlungsvorgangs nicht per Internet übermittelt werden. Mit paybox (http://www.paybox.de) ist ein solches Zahlungssystem schon weit verbreitet, während ein vergleichbares System wie TeleCash (http://www.telecash.de) noch in den Anfängen steckt.

Insbesondere zur Bezahlung kleiner Beträge sind Micropaymentsysteme wie infin-MicroPayment (http://www.infin.de) vorgesehen, bei denen das Inkasso durch einen Dritten, etwa die Deutsche Telekom AG, erfolgt. Der Anbieter einer Dienstleistung gibt

im Internetangebot beispielsweise eine 0190er-Telefonnummer bekannt, über die der Nutzer eine Transaktionsnummer erhält, mit der er das Angebot freischalten kann. Datenschutzrechtlich relevant ist die Tatsache, dass der Nutzer gegenüber dem Anbieter anonym bleibt, die Telekom hingegen lediglich Namen und Telefonnummer, nicht aber die in Anspruch genommene Dienstleistung kennt. Das Prinzip der Datensparsamkeit ist hier durch die Verteilung des Wissens gut umgesetzt.
Wiederum andere Bezahlverfahren erfordern eine spezielle Software auf dem Rechner des Nutzers. Möchte der Kunde ein kostenpflichtiges eGovernment-Angebot nutzen, so beendet der Client automatisch die bestehende Internetverbindung. Die Software baut dann eine speziell tarifierte Verbindung zum Inkasso-Server auf, überträgt den Gebührendatensatz und aktiviert danach wieder die ursprünglichen Internetverbindung. Nach diesem Prinzip funktioniert beispielsweise das Verfahren Net900 der Telekom (http://www.in-medias-res.com), mit dem vorwiegend Kleinstbeträge über die Telefonrechnung beglichen werden sollen. Nutzerrelevante Daten liegen nur beim Inkassounternehmen vor und die Anonymität des Nutzers gegenüber dem eGovernment-Anbieter bleibt gewahrt. Das Verfahren ist unter dem Gesichtspunkt der Datenvermeidung positiv zu bewerten.

5.7.7 Dokumentenmanagement

Sind die Schriftstücke elektronisch abgelegt, ermöglichen elektronische Dokumentenverwaltungssysteme den schnellen, ungehinderten Online-Zugriff auf die Inhalte jedes einzelnen Dokumentes von jedem angeschlossenen Arbeitsplatz. Dabei kann das Wiederauffinden von Dokumenten durch vielfältige Suchfunktionen unterstützt werden. Da die elektronischen Archivierungssysteme jedes Dokument gesondert erfassen, gehören Akten im klassischen Sinne (d.h. als physikalisch verbundene Dokumentensammlungen, die über ein einheitliches Kriterium – Aktenzeichen – erschlossen werden) der Vergangenheit an. Die „elektronische Bürgerakte“ ist vielmehr rein virtuell, d.h. eine durch logische Zuordnungskriterien gebildete Datenzusammenstellung, wobei dasselbe Dokument zugleich Bestandteil verschiedener Akten sein kann. Es ist klar, dass diese übergreifenden Zuordnungs- und Auswertungsmöglichkeiten erhebliche Auswirkungen auf den Datenschutz haben.

Handlungsempfehlungen:

- ☞ Personenbezogene Daten dürfen nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Datenbestand, etwa in einer elektronischen Sachakte, muss daher zum frühestmöglichen Zeitpunkt gelöscht oder zumindest gesperrt werden, wenn der ursprüngliche Verwendungszweck der Speicherung erfüllt ist.
- ☞ Gestaltung und Auswahl von Dokumentmanagement-Systemen haben sich an dem Ziel auszurichten, bei der Speicherung, Nutzung und Protokollierung so wenig personenbezogene Daten wie möglich zu verarbeiten.
- ☞ Auswertungen mit Data-Mining-Instrumenten sind grundsätzlich nur anonym oder pseudonym zulässig (Gefahr von Profilbildung).
- ☞ Betroffene sind umfassend zu unterrichten, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können.

- ☞ Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig.
- ☞ Für die Betriebssystemebene und für die Anwendung sowie für die Auswertung und die Statistiken des Datenbestandes ist ein Berechtigungs- und Zugriffskonzept festzulegen.
- ☞ Protokollierungen und Kontrollen sind festzulegen.
- ☞ Anforderungen an die Speicherung und die langfristige Aufbewahrung elektronischer Dokumente sind festzulegen.
- ☞ Der Einsatz einer elektronischen Signatur und die Verschlüsselung der gespeicherten Daten sind in Abhängigkeit des Schutzbedarfs vorzusehen.
- ☞ Eingangs- und Ausgangsschnittstellen zu anderen Verfahren sind inhaltlich und technisch zu dokumentieren.
- ☞ Ein Sicherheitskonzept und eine Dienstanweisung sollten erstellt werden.

5.7.8 Protokollierungen der Nutzung

Mit der Protokollierung der Verarbeitung entstehen auf allen drei Ebenen (siehe Abschnitt 3.5) Sammlungen personenbezogener Daten. Damit wird es z.B. möglich, Nutzerprofile abzuleiten oder Listen über Auffälligkeiten zu erstellen.

Handlungsempfehlungen:

- ☞ Erhebung, Verarbeitung und Weitergabe von personenbezogenen Daten (Bestands-, Verbindungs- und Nutzungsdaten) sollten grundsätzlich anonymisiert oder mittels eines Pseudonyms erfolgen.
- ☞ Für Art, Umfang und Aufbewahrung der Protokollierung und Bestandsdaten gilt der Grundsatz der Erforderlichkeit.
- ☞ Protokolldaten dürfen nur zu Zwecken genutzt werden, die Anlass für ihre Speicherung waren.
- ☞ Die Daten über die Inanspruchnahme verschiedener Online-Dienste werden getrennt gespeichert.
- ☞ Eine unzulässige Zusammenführung der Nutzungsdaten ist technisch zu verhindern.
- ☞ Die Protokolldaten werden bei kostenfreier Nutzung des Online-Dienstes nach Ende der jeweiligen Nutzung gelöscht; bei kostenpflichtiger Nutzbarkeit sind die Protokolldaten spätestens nach Ablauf von sechs Monaten nach Versendung der Rechnung und des Einzelnachweises zu löschen, soweit es nicht zu Einwendungen gekommen ist oder nach bereichsspezifischen Regelungen besondere Aufbewahrungsfristen zu beachten sind.
- ☞ Die Verwendung von Protokolldaten zu Zwecken der Verhaltens- und Leistungskontrolle ist untersagt. Nur im Einzelfall ist eine Auswertung der Protokolldaten zur Aufdeckung von Missbräuchen zulässig.

Siehe hierzu auch Kapitel 6.2.3.

5.7.9 Einschaltung Dritter

Beauftragt eine Behörde ein privates Dienstleistungsunternehmen oder einen anderen Dritten, um für sie Hardware, Software oder auch Tele- und Mediendienste zu betreiben und zu warten (Outsourcing), so ist dabei auf folgende Punkte zu achten:

Handlungsempfehlungen zur Vertragsgestaltung

- ☞ Der Auftragnehmer sollte kein eigenes, fachlich bestimmtes Interesse an einem Zugriff auf Inhaltsdaten haben (Eingrenzung der Gefahr eines Datenmissbrauches).
- ☞ Bereits bei der Auswahl des Auftragnehmers ist darauf zu achten, dass er die erforderlichen technischen und organisatorischen Maßnahmen ergreifen kann. Das setzt voraus, dass alle wesentlichen Anforderungen bekannt sein müssen und sich der Auftraggeber davon überzeugt hat, dass der Auftragnehmer in der Lage ist, diese umzusetzen, bevor der Auftragnehmer erstmals Gelegenheit erhält, auf personenbezogene Echtdaten zuzugreifen.
- ☞ Den Regeln der Auftragsdatenverarbeitung entsprechend, muss für jedes Outsourcing-Vorhaben ein schriftlicher Auftrag erteilt werden. Darin sind
  - Rechte und Pflichten der Daten verarbeitenden Stelle und des Fernwartungsunternehmens detailliert festzulegen,
  - Gegenstand und der Umfang der übertragenen Tätigkeiten,
  - die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Datenschutzmaßnahmen sowie
  - etwaige Unterauftragsverhältnisse

  darzustellen.
- ☞ Ferner muss vereinbart werden, dass der Auftraggeber dem Auftragnehmer Weisungen hinsichtlich der Verarbeitung personenbezogener Daten erteilen darf.
- ☞ Das Personal des beauftragen Unternehmens ist auf das Datengeheimnis (z. B. nach § 5 BDSG) zu verpflichten.
- ☞ In der Vereinbarung ist ferner festzulegen, dass der Auftragnehmer sich der Kontrolle der zuständigen staatlichen Datenschutzaufsichtsbehörde unterwirft; dabei sind die Vorgaben des jeweils einschlägigen Datenschutzgesetzes zu beachten.
- ☞ Vor allem bei größeren Projekten bietet es sich an, die technisch-organisatorischen Maßnahmen in einem Datenschutz- und Sicherheitskonzept zusammenzufassen, dessen Umsetzung und Einhaltung vertraglich vereinbart wird. Die technisch-organisatorischen Maßnahmen können dann dem Stand der Technik folgend fortgeschrieben werden, ohne dafür den Outsourcing-Vertrag selbst ändern zu müssen.

Weitere Handlungsempfehlungen zu den technischen Vorkehrungen bei der Einschaltung Dritter finden Sie unter 6.2.4.

5.7.10 Informationsfreiheit, Zugang zu öffentlichen Informationen

Will eine öffentliche Stelle die bei ihr vorhandenen Informationen elektronisch zur Verfügung stellen, muss sie sich zunächst darüber Gedanken machen, über welche Art von Informationen sie verfügt und in welchem Umfang bzw. unter welchen Voraussetzungen diese zugänglich gemacht werden können. Voraussetzung ist also, die gespeicherten Informationen zu klassifizieren.

Dabei bietet es sich an, die Informationen nach dem Grad ihrer Vertraulichkeit einzuteilen, da hiervon in aller Regel abhängt, inwieweit ein Zugang der Öffentlichkeit zu diesen Informationen besteht. Sieht man von Informationen ab, die unter keinen Voraussetzungen zugänglich gemacht werden können, kommen danach im Wesentlichen zwei Kategorien von Informationen in Betracht:

Kategorie 1:

Informationen, die unabhängig vom Vorhandensein eigener Informationsfreiheitsgesetze öffentlich zugänglich gemacht werden können und/oder ohnehin öffentlich bekannt gemacht werden müssen. Dazu zählen z. B. Verlautbarungen in Amtsblättern, Beschlüsse kommunaler Vertretungskörperschaften, kommunale Satzungen, Bauleitpläne, aber auch Geschäftsverteilungspläne (ohne Nennung der Namen der Bediensteten) oder Informationen über die Erreichbarkeit der öffentliche Stelle.

Kategorie 2:

Informationen, die nach den Informationsfreiheits- oder anderen Spezialgesetzen grundsätzlich nur auf Antrag zugänglich sind und in der Regel aus dem laufenden Verwaltungsvollzug stammen. Hierbei kann noch einmal unterschieden werden zwischen Informationen mit (zumindest teilweise) geheimhaltungsbedürftigem Inhalt und solchen ohne derartige Inhalte. Die Geheimhaltungsbedürftigkeit kann sich daraus ergeben, dass die Vorgänge personenbezogene Daten, zu schützende Betriebs- oder Geschäftsgeheimnisse oder aus öffentlichem Interesse geheimzuhaltende Informationen enthalten.

Handlungsempfehlungen zu Kategorie 1:

- ☞ Die Dokumente können in elektronischer Form ohne weiteres vollständig in das Internet eingestellt, d. h. auf einem Webserver der öffentlichen Stelle gespeichert werden. Es empfiehlt sich schon bei der Erstellung der Dokumente möglichst weit verbreitete Dateiformate zu wählen, die mit handelsüblichen Browsern oder verbreiteter möglichst kostenloser Software (Freeware) von den Bürgerinnen und Bürgern ohne weiteres gelesen werden können. Hierfür bieten sich insbesondere das HTML- oder das PDF-Format an.
- ☞ Die Dokumente sollten strukturiert so abgelegt werden, dass das Prinzip der Ablage für die Nutzer transparent ist. Empfehlenswert ist, intelligente Suchmaschinen in das Angebot zu integrieren, die das Auffinden der Dokumente erleichtern.
- ☞ Da es sich um Informationen handelt, die jedermann öffentlich zugänglich sind, spielt die Identität des Abfragenden keine Rolle. Der Informationszugang ist hier also anonym zu gewähren. Aus dem gleichen Grunde ist eine besondere Absicherung der Kommunikation selbst durch Verschlüsselung der übertragenen Daten nicht zwingend erforderlich.
- ☞ Nach den Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) sowie des Mediendienste-Staatsvertrages (MDStV) sind Nutzungsdaten spätestens mit Ende der Nutzung zu löschen, da das Internet-Angebot hinsichtlich dieser Informationen kostenfrei ist und die Identität der Nutzer keine Rolle spielt. Insbesondere dürfen keine IP-Adressen erfolgter Zugriffe in Log-Dateien gespeichert werden.
- ☞ Die Verwaltung muss sich – anders als der Nutzer – ihrerseits eindeutig identifizieren, damit die Nutzer sicher sein können, dass die Informationen von einer öffentlichen Stelle stammen.

Handlungsempfehlungen zu Kategorie 2

- ☞ Es muss ein logisch aufgebauter und für die Nutzer transparent strukturierter Aktenplan geschaffen werden. Der Aktenplan sollte daher nach solchen Stichworten gegliedert sein, unter denen die Bürgerinnen und Bürger die dahinter abgelegten Vorgänge auch vermuten würden. Es bietet sich an, einen kommentierten Aktenplan nach Art eines Behördenwegweisers oder Leitfadens für die Bürger zu entwerfen.
- ☞ Die zur Einsicht bestimmten Dokumente, ggf. unter Einbeziehung der Dokumente aus Fachverfahren, sind in ein einheitliches Format zu bringen. Denkbar ist auch, bereits im lokalen Netzwerk (LAN) Produkte zu implementieren, die einen differenzierten Zugriff auf die vorhandenen Daten mittels Browser nach dem XML-Standard ermöglichen. In jedem Falle muss – schon aus Datenschutzgründen – technisch sichergestellt werden, dass von außen wie von innen nur zweckgebundene differenzierte Zugriffe möglich sind.
- ☞ Zusätzlich zum Workflow beim Output der Informationen muss auch der Workflow beim Input (Eingang des Antrages auf Informationszugang) in der Verwaltung auf elektronische Art und Weise gewährleistet und in der Verwaltungsorganisation berücksichtigt werden.
- ☞ Es müssen die geeigneten technischen und organisatorischen Voraussetzungen für ein Dokumentenmanagement-System geschaffen werden.
- ☞ Eine zweifelsfreie Identifizierung des Antragstellers ist jedenfalls dann erforderlich, wenn die Informationen auf Antrag im Einzelfall bereitgestellt werden. Die Gewährung des Zugangs und dessen Ablehnung ist in diesen Fällen ein Verwaltungsakt, der schon wegen der möglichen Rechtsmittel dem Antragsteller zugestellt werden muss. Außerdem muss nach den Informationsfreiheitsgesetzen in einigen Fällen die Zustimmung Dritter eingeholt werden, deren Erteilung für den Dritten durchaus von der Identität des Antragstellers abhängen kann.
- ☞ Soweit die Vorgänge Informationen enthalten, die aus überwiegendem öffentlichen oder privatem Interesse geheim zu halten sind, müssen technische und organisatorische Voraussetzungen geschaffen werden, geheimhaltungsbedürftige Dokumente elektronisch auszusondern, da die Informationsfreiheitsgesetze dies in der Regel dann vorschreiben, wenn es ohne erheblichen Aufwand möglich ist. Deshalb ist bereits beim Anlegen elektronischer Akten darauf zu achten, dass z.B. personen- oder geheimhaltungsbedürftige unternehmensbezogene Dokumente so abgelegt oder gekennzeichnet werden, dass das Aussondern ohne großen Aufwand möglich ist. Insofern bietet eine eGovernment-Lösung aber auch Chancen für ein zugangsfreundliches Dokumentenmanagement.
- ☞ Soweit – mit Zustimmung der Betroffenen – personenbezogene Daten übertragen werden sollen, ist eine Verschlüsselung der Daten nach dem Stand der Technik erforderlich.
- ☞ Soweit der Informationszugang gebührenpflichtig ist, bietet es sich an, zur Bezahlung der Gebühren ein elektronisches Zahlungsverfahren in das Angebot zu integrieren, um einen Medienbruch zu vermeiden. Dabei sollte datenschutzfreundlichen Verfahren der Vorrang gewährt werden. So ist eine Identifizierung konkreter Personen in vielen Fällen nicht erforderlich (siehe Kapitel 5.7.6).

☞ Die Integration eines elektronischen Informationszugangs in den laufenden Verwaltungsablauf stellt auch die Mitarbeiterinnen und Mitarbeiter vor neue Herausforderungen bei der Führung von Akten. Ein umfassender Zugang zu Informationen ist ohne entsprechende Motivation der Beschäftigten daher nicht denkbar.

6 Baukasten für technisch-organisatorische Werkzeuge

6.1 Systemdatenschutz

Durch eine gezielte Gestaltung der Systeme und Verfahren zur Verarbeitung personenbezogene Daten soll erreicht werden, dass die Ziele des Datenschutzrechts durch die Technik selbst gewährleistet werden. Durch Systemsdatenschutz sollen

- Datenschutzrisiken durch Maßnahmen zur Datenvermeidung und Datensparsamkeit reduziert,
- infomationelle Gewaltenteilung durch Verteilung von Verarbeitungsprozessen, und Datenbeständen verwirklicht,
- die Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit der Daten durch Maßnahmen der Datensicherheit gewährleistet und
- die infrastrukturellen Voraussetzungen für Selbstdatenschutz (s. Kapitel 6.3) geschaffen werden.

6.1.1 Architekturmodell

Anwendungsübergreifende Lösung

Für eGovernment sollten Lösungen auf einer einheitlichen anwendungsübergreifenden technischen Plattform entwickelt werden. Diese sollte modular aufgebaut sein, sodass mehrere Anwendungen parallel und unabhängig voneinander betrieben werden können. Auch sollte sie weitestgehend Möglichkeiten zur Erweiterung und Anwendung zusätzlicher Verfahren bieten. Dies bedeutet neben finanziellen auch datensicherheitsrelevante und administrative Vorteile. Weiterhin wird durch den Einsatz einer einheitlichen Technik der Aufwand an Hardware, Software, Lizenzen und Ausbildung minimiert. Die Konfiguration des Internetzugangs wird vereinfacht, da durch eine Vereinheitlichung der bei den Anwendungen verwendeten Dienste die Anzahl der potentiellen Schwachstellen minimiert wird. Das Gesamtsystem ist allerdings nur so sicher wie sein schwächstes Element, deshalb sind bei der Kompromittierung einer Anwendung alle anderen Anwendungen ebenfalls betroffen. Bei der Verwendung einer einheitlichen Lösung ist der Betrieb, das Monitoring eventueller Angriffe, die Reaktion auf neue Sicherheitslücken und die Implementierung neuer Maßnahmen somit bedeutend einfacher. Auch wenn es unterschiedliche Sicherheitsbedürfnisse für die Anwendungen geben mag, so lassen sich durch die Implementierung des ohnehin notwendigen höchstmöglichen Sicherheitsniveaus die Anforderungen aller Anwendungen erfüllen. Eine nachträgliche Erhöhung des Sicherheitsstandards ist ebenfalls bedeutend einfacher, im Gegensatz zu einer Situation, in der mehrere unterschiedliche Ansätze betrachtet und aufwändig erneuert werden müssen. Die Voraussetzungen für eine gemeinsame Plattform für eGovernment-Anwendungen sind bereits in vielen Dienststellen gegeben.

Anwendungsspezifische Lösung

Alternativ zur Implementierung einer anwendungsübergreifenden Gesamtlösung besteht die Möglichkeit der Realisierung der Verfahren als einzelne Anwendungen, die in die bestehende Systemarchitekturen integriert sind. Diese Vorgehensweise erlaubt die Verwendung der bereits angeschafften Anwendungen. Als nachteilig ist allerdings ein generell höherer Aufwand für den Betrieb und die Wartung zu sehen. Da als allgemeine Vorgabe die Einhaltung von Sicherheitsstandards auf dem Niveau des Signaturgesetzes angestrebt werden sollte, sind allerdings für die Produkte jeweils noch Erweiterungen nötig. Problematisch kann sich auch die Inanspruchnahme von Supportdienstleistungen gestalten, vor allem, wenn eine Fehlerquelle unklar ist oder sich nur schwer ermitteln lässt. Es sollte ebenfalls die Vorgehensweise beim Upgrade einer Anwendung mit den Lieferanten geklärt werden, um auszuschließen, dass Updates nicht installierbar sind.

6.1.2 Produktentwicklung unter Berücksichtigung der Common Criteria

Bei komplexen eGovernment-Anwendungen ist sehr schwer zu beurteilen, in welchem Umfang und auf welche Weise personenbezogene Daten verarbeitet werden. Die Nutzer der Informationstechnik müssen jedoch darauf vertrauen können, dass die notwendigen Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden. Um die Sicherheitseigenschaften von IT-Produkten vergleichen und das Maß der Vertrauenswürdigkeit einschätzen zu können, haben verschiedene Länder Europas und Nordamerikas die so genannten Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) entwickelt. Die Common Criteria 2.0 enthalten unter anderem auch Anforderungen zum Schutz der Privatsphäre. Mit Hilfe der in den Common Criteria beschriebenen Schutzprofile (Protection Profiles) können somit datenschutzspezifische Anforderungen für bestimmte Produkttypen definiert werden. Dadurch ist es einerseits möglich, Herstellern von IT-Produkten international vergleichbare und – insbesondere für die Produktzertifizierung – prüffähige Vorgaben für die Entwicklung datenschutzfreundlicher Produkte zu machen. Andererseits können Zertifizierungsstellen solche Produkte evaluieren und prüfen. Anbieter von eGovernment-Dienstleistungen werden somit in die Lage versetzt, das Maß an Datenschutzfreundlichkeit ihrer Anwendungen bereits vor dem Einsatz selbst zu bestimmen und im späteren Einsatz objektiv einzuschätzen.

Seit dem 11. November 2002 bietet der Bundesbeauftragte für den Datenschutz zwei derartige, international anerkannte Schutzprofile an (Titel: BISS - Benutzerbestimmbare Informationsflusskontrolle, Registrierungskennzeichen: BSI-PP-0007-2002 und BSI-PP-0008-2002; http://www.bfd.bund.de/technik/protection_profile.html). Kerngedanke der in den Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Diese Regeln (z. B. verschlüsselte Speicherung, verschlüsselte Übertragung, signierte Übertragung) können aus rechtlichen, organisatorischen und technischen Rahmenbedingungen abgeleitet und vom Anwender vorgegeben werden.

Vor diesem Hintergrund sollten künftige Anbeiter von eGovernment-Dienstleistungen vor jeder Produktentwicklung überlegen, ob sie ihre Datenschutz- und Sicherheitsanforderung beispielsweise mit Hilfe der oben genannten Schutzprofile beschreiben

können, um sie nach Abschluss der Entwicklung von unabhängigen Prüfinstitutionen nach international gültigen Kriterien prüfen zu lassen.

6.1.3 Kryptographische Verfahren

Durch den Einsatz kryptographischer Verfahren können wesentliche datenschutzrechtliche und sicherheitstechnische Ziele erreicht werden. So kann durch Verschlüsselung die Vertraulichkeit gespeicherter bzw. übermittelter Daten sichergestellt werden, d.h. dass nur Befugte den Inhalt der Nachricht bzw. der Datei zur Kenntnis nehmen können. Kryptographie ist somit auch ein wichtiges Werkzeug zur Wahrung der Zweckbindung in eGovernment-Projekten. Weiterhin sind bestimmte kryptographische Verfahren geeignet, unbefugte Manipulationen an Nachrichten oder Dateien zu verhindern bzw. nachträglich aufzudecken und somit die Integrität zu gewährleisten. Auch zur Authentisierung von Kommunikationspartnern wird Kryptographie eingesetzt, damit Personen, Organisationen und IT-Systeme gegeneinander ihre Identität zweifelsfrei beweisen können. Darüber hinaus gestatten diese Verfahren den Nachweis der Herkunft und des Empfangs von Nachrichten.
Bei der Auswahl kryptographischer Verfahren ist grundsätzlich darauf zu achten, dass sie für verschiedene Betriebssysteme und Serverplattformen zur Verfügung stehen (Interoperabilität) und dass die verwendeten Algorithmen dem Stand der Technik entsprechen (siehe hierzu die regelmäßigen Bekanntmachungen des BSI). Von besonderer Bedeutung für die Sicherheit kryptographischer Verfahren ist eine ausreichende Schlüssellänge und ein angemessenes Schlüsselmanagement. Detaillierte Hinweise hierzu enthält beispielweise der Abschnitt 3.7 (Kryptokonzept) des IT-Grundschutzhandbuchs des BSI.
Darüber hinaus hat der KoopA-ADV als Arbeitshilfe einen Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung für die öffentliche Verwaltung (http://www.koopa-adv.de/Arbeitsgruppen /Kommunikation/ KoopAgesamt.pdf) entwickelt, der Lösungen für die Entwicklung kryptographischer Szenarien aufzeigt.
Mit dem Online Service Computer Interface (OSCI) steht ein speziell für eGovernment-Anwendungen entwickelter Protokoll-Standard zur Verfügung, dessen Basis verschiedene kryptographische Verfahren sind. Als sicheres Übertragungsprotokoll soll OSCI rechtsverbindliche und signaturgesetzkonforme Online-Transaktionen ermöglichen. Durch eine sinnvolle Kombination von Verschlüsselungen wird der Aufbau sicherer Verwaltungsportale unterstützt, sodass den eGovernment-spezifischen Bedrohungen (siehe Abschnitt 4.1) wirksam begegnet werden kann. Die bremen online services GmbH & Co. KG stellt mit der Architektur Governikus eine Signatur-Anwendungskomponente zur Verfügung, die auf dem OSCI-Standard basiert.
Im folgenden Abschnitt sind Maßnahmen beispielhaft beschrieben, die zum Erreichen grundlegender Datensicherheitsziele geeignet sind. Neben vielen anderen Einzelmaßnahmen sind kryptographische Verfahren besonders wichtige Hilfsmittel. Ausführliche Hinweise zu diesem Thema sind unter anderem im eGovernment-Handbuch des BSI, Kapitel „Kryptographie im Internet“, zu finden.

6.1.4 Maßnahmen zur Gewährleistung der Datensicherheit

Vertraulichkeit übermittelter Daten

Um die Vertraulichkeit von Informationen zu sichern, die beispielsweise ein Bürger aus dem eGovernment-Angebot der Behörde abruft, bietet sich die Nutzung des Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protokolls an, das eine verschlüsselte Datenübertragung zwischen Server und Client sicherstellt. Aufgrund der Verschlüsselung sind sowohl abgerufene Inhalte des Servers als auch Datenübertragungen des Nutzers, etwa Eingaben in Webformulare, für Unbefugte nicht einsehbar.

Integrität des Angebotes

Die Nutzung des SSL/TLS-Protokolls schützt auch gegen eine Veränderung der Daten auf dem Transportweg. Elektronische Signaturen und Prüfsummen ermöglichen, dass Veränderungen nachträglich feststellbar sind. Die Integrität der Daten auf dem Server muss ggf. durch ergänzende Maßnahmen wie etwa Zeitstempel sichergestellt werden.

Authentizität der Kommunikationspartner

In Abhängigkeit vom angebotenen Service und der Funktionalität kann es notwendig sein, dass sich der Nutzer gegenüber dem Behördenserver identifiziert, etwa wenn Daten nur an besonders berechtigte Nutzer übertragen werden dürfen. Je nach der Art des eGovernment-Angebots und nach dem Umfang der beteiligten Personenkreise können folgende Maßnahmen zum Einsatz kommen:

- Für geschlossene Benutzergruppen:
  - Authentisierung durch Login- und Passwortvergabe.
- Für offene Benutzergruppen:
  - signaturgesetzkonforme elektronische Signaturen (fortgeschrittene oder qualifizierte in Abhängigkeit vom jeweiligen Schutzbedarf),
  - Authentisierungsserver, der die erforderlichen Authentisierungsdaten zentral vorhält und von der Arbeitsstation übermittelte Passwörter auf Richtigkeit prüft,
  - Einsatz so genannter elektronischer Ausweise (vgl. Roßnagel, Der Elektronische Ausweis, DuD 26 (2002) 5, S. 281-285).
- Für institutionelle Nutzer (Angehörige eines Unternehmens oder einer Behörde) ist durch zusätzliche Maßnahmen, etwa Client-Zertifikate sicherzustellen, dass nur Berechtigte aus der Institution auf die Datenbestände zugreifen können.

Bei jeder eGovernment-Anwendung ist zu prüfen, ob die Identifizierung der Nutzer tatsächlich erforderlich ist oder ob das Angebot auf pseudonyme oder anonyme Weise genutzt werden kann. Beim Download von Anträgen von einem Behördenserver ist beispielsweise die Identität des Nutzers ohne Belang. Selbst bei kostenpflichtigen Angeboten ist die Preisgabe der Identität des Nutzers nicht notwendig, wenn Methoden zur anonymen Zahlung zum Einsatz kommen (Beispiele für Zahlungssysteme siehe Kapitel 5.7.6).
Zur Authentisierung des Angebotsservers bietet sich wiederum das Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protokoll an, das mit Hilfe von Zertifikaten die Authentisierung des Servers gegenüber dem Client ermöglicht.

Verfügbarkeit des Angebotes

Um die Verfügbarkeit der angebotenen Inhalte und Dienste zu gewährleisten, müssen Maßnahmen gegen Datenverluste, technische Ausfälle und Sabotage (etwa Angriffe gegen die Integrität des Servers oder so genannte Denial-of-Service (DoS)-Angriffe) getroffen werden. Die im Abschnitt 6.2.3 beschriebenen Maßnahmen zur Revision (siehe insbesondere Protokollierung) sind auch geeignet, um Angriffe nachträglich festzustellen. Neben der Realisierung von Datensicherungsmaßnahmen (siehe Abschnitt 6.2.2), einer unterbrechungsfreien Stromversorgung und ausreichender Klimatisierung gehört auch die Fähigkeit, auf Sicherheitsvorfälle schnell und angemessen reagieren zu können, zu diesem Komplex.

6.1.5 Gestaltung des Web-Angebots

Aktive Inhalte

Auf aktive Inhalte (etwa ActiveX-Controls, Java- und JavaScript-Funktionen oder Plug-Ins) sollten Anbieter von eGovernment-Angeboten verzichten, weil davon auszugehen ist, dass die Nutzer aktive Inhalte wegen ihrer Sicherheitsprobleme restriktiv nutzen, indem sie beispielsweise die entsprechenden Funktionen im Browser deaktivieren (siehe Abschnitt 6.3 und Orientierungshilfe Internet des AK Technik, Abschnitt 2.3.3). Anbieter sollten Nutzer nicht mit einer datenschutzunfreundlichen Gestaltung ihrer Angebote zwingen, aktive Inhalte zu nutzen oder Plug-Ins zweifelhafter Herkunft zu installieren.
Sollte im Einzelfall die Verwendung von Java sinnvoll erscheinen, etwa bei der Gestaltung von Formularsätzen und Eingabefeldern, sollten ausschließlich solche Java-Applets und Javascripts verwendet werden, die mit einer elektronischen Signatur versehen und somit vom Nutzer prüfbar sind. Den Nutzern ist in diesen Fällen zu empfehlen, die Ausführung aktiver Inhalte sofort nach Verlassen des Internet-Angebots der Behörde in ihren Browsern wieder zu deaktivieren. Auf andere Arten von aktiven Inhalten (insbesondere ActiveX-Objekte, VBscripts) sollte in jedem Fall verzichtet werden. Weitere Hinweise zum Umgang mit aktiven Inhalten enthält das eGovernment-Handbuch des BSI, Kapitel „Sicherer Internet-Auftritt im eGovernment“, Abschnitt 7.

Die eGovernment-Angebote von Behörden sollten weitgehend auf Cookies verzichten. Es sollten höchstens temporäre Cookies (sog. Sessions-Cookies) zum Einsatz kommen. Zwar gibt es seit jüngerer Zeit recht wirkungsvolle Mechanismen, den Zugriffs auf Cookies für den Benutzer transparent und kontrollierbar zu halten (vgl. Abschnitt 6.3), doch sind diese (noch) nicht sehr weit verbreitet. Daher wird den Nutzern häufig die Deaktivierung der Cookie-Funktionalität empfohlen (vgl. Orientierungshilfe Internet des AK Technik, Abschnitt 2.3.3.5).

Dynamische Seiten

Während aktive Inhalte Risiken für den Bürger bedeuten, stellen dynamische Internet-Seiten Gefährdungen für den Betreiber dar. Um diesen Gefahren zu begegnen, sollten dynamische Seiten mit Reaktion auf Benutzereingaben nur sparsam verwendet werden. Die verwendeten Scripte sind sorgfältig vor dem Einsatz zu überprüfen, insbesondere hinsichtlich ihrer Resistenz gegen Fehleingaben. Zur Suche von Sicher-

heitslücken kann die Protokollierung der Eingaben sinnvoll sein (zu einzelnen Maßnahmen vgl. eGovernment-Handbuch, Kapitel „Sicherer Internet-Auftritt im eGovernment“, Abschnitt 8).

6.1.6 Schutz des Web-Angebots und der Infrastruktur des Anbieters

Einsatz von Firewalls

Das Webangebot sollte grundsätzlich durch ein geeignetes Firewallsystem abgesichert werden. Zwar lässt sich ein minimaler Schutz auch durch die Einrichtung von Filterlisten auf dem Router, der dem Angebot direkt vorgeschaltet ist, erreichen. Die Sicherheitssoftware der Router-Hersteller kann jedoch nur einen Teil der möglichen Angriffe herausfiltern. Komplexere Angriffe könnten deshalb Erfolg haben. Da die Router-Software in der Regel keine Alarmierungsfunktion bei Angriffen vorsieht, ist diese Variante des minimalen Schutzes des Webangebotes für Behörden nicht empfehlenswert.
Die Leistungsfähigkeit der eingesetzten Firewall muss sich sowohl an der Schutzbedürftigkeit der Daten (siehe dazu Abschnitt 6.2.1 Sicherheitskonzept) als auch an den möglichen und erlaubten Kommunikationsbeziehungen zwischen Nutzer, Angebotsserver und evtl. Behörde orientieren. Ein Webserver, der ein reines Informationsangebot bereitstellt, ist sicherlich weniger schutzbedürftig als ein Server, der zusätzlich amtliche Formulare bereithält oder sogar die rechtsverbindliche Weitergabe von ausgefüllten Formularen an die Behörde zulassen soll. Grundsätzlich sollte nur das notwendige Minimum an Diensten zugelassen werden.
Ein Firewallsystem ist grundsätzlich als "gehärtetes System" aufzusetzen, bei dem nur die Betriebssystemkomponenten installiert werden, die zum Betrieb der Firewall wirklich benötigt werden. Alle weiteren Komponenten und Services sollten deaktiviert oder erst gar nicht installiert werden. Alle nicht benötigten Benutzerzugänge sind zu löschen, da sie unnötige Angriffspunkte darstellen.
Detaillierte Informationen zu Firewalls, Firewallkonzepten und Policies enthält unter anderem das eGovernment-Handbuch des BSI (insbesondere in den Abschnitten 2 und 3 des Kapitels „Sicherer Internet-Auftritt im eGovernment“) oder die Orientierungshilfe Internet des AK Technik, Kapitel 3 Firewallsysteme.

Log-Dateien auf Webserver und Firewall

Das Firewallsystem und das darunter liegende Betriebssystem sollten weitgehend revisionssicher ausgestaltet werden. Dazu gehört neben einem "journaling Filesystem", mit dem Veränderungen an wichtigen Konfigurationsdateien nachvollzogen werden können, das Protokollieren sämtlicher Systemveränderungen bis hin zum Ein- bzw. Ausloggen der Administratoren und den von ihnen abgesetzten Befehlen. Die dabei entstandenen System-Log-Dateien müssen der Behörde während der Aufbewahrungsfrist zur Verfügung stehen.
Es ist technisch prinzipiell möglich, neben der Protokollierung der Administrationstätigkeiten auch die gesamte Kommunikation mit dem Webserver sehr detailliert durch die Firewall oder den Webserver selbst zu protokollieren.
Datenschutzrechtlich unproblematisch sind Verkehrs-Log-Dateien, die zum Beispiel der Optimierung des Webserver-Angebotes dienen, sofern folgende Randbedingungen eingehalten werden:

- lediglich statistische Auswertung der Protokolle,
- Anonymisierung der Logdaten z. B. durch gezielte Veränderung der IP-Adressen,
- Auswertung der Daten innerhalb von 3 Werktagen,
- Löschen der Verkehrs-Log-Dateien sofort nach der Auswertung.

Fraglich ist, welchen Nutzen personenbezogene Firewall-Logfiledaten**,** etwa im Falle eines Angriffs auf das Angebot, bieten. Bei einem sorgfältig konzipierten, installierten und administrierten Firewallsystem wird ein Angriff mit hoher Wahrscheinlichkeit abgewehrt werden. Wenn gleichzeitig der entsprechende Eskalationsplan in Gang gesetzt wird und lediglich die aus dem Zeitraum des Angriffs stammenden Daten zur späteren Analyse aufbewahrt werden, ist die längerfristige Aufbewahrung aller Logfile-Daten nicht erforderlich. Sinnvoll wäre hier höchstens die regelmäßige Auswertung der Daten durch ein Skript mit festgelegten Regeln oder der Einsatz eines Intrusion Detection Systems. Die unreflektierte Aufbewahrung sämtlicher Logfiledaten führt zu einer immensen Datenhaltung und ist nicht mit den Grundsätzen der Datensparsamkeit zu vereinbaren. Zur Zulässigkeit der Protokollierung und zu Fragen der Inhaltskontrolle an Firewalls informiert die Orientierungshilfe Internet des AK Technik im Kapitel 4 ausführlich.

Infrastrukturelle Maßnahmen der Behörde

Als infrastrukturelle Sicherungsmaßnahmen kommen grundsätzlich die in Kapitel 4 des IT-Grundschutzhandbuches des BSI zur Absicherung von Gebäuden und Räumen genannten Maßnahmen in Betracht. In Abhängigkeit von der konkreten Gefährdungslage vor Ort sind einzelne Maßnahmen auszuwählen, im Sicherheitskonzept (siehe Abschnitt 6.2.1) zu dokumentieren und gegebenenfalls nach einem konkreten Zeitplan umzusetzen.

Zusätzliche Maßnahmen bei verschiedenen Umsetzungsvarianten

In Abhängigkeit von Art und Umfang des eGovernment-Angebots sowie der personellen und finanziellen Möglichkeiten des Anbieters sind verschiedene Formen der Angebots-Bereitstellung denkbar. Neben den o. g. allgemein gültigen Maßnahmen sind in der Regel weitere Schutzvorkehrungen erforderlich, die unter anderem auch von der Art der Einbeziehung externer Dienstleister abhängen. Im Folgenden werden drei unterschiedliche Varianten betrachtet.

<u>eGovernment-Server beim Dienstleister</u>
Wird der eGovernment-Server nicht beim Anbieter (der Behörde) selbst, sondern bei einem Dienstleister untergebracht, unterscheidet man allgemein zwischen "Hosting" und "Housing". Beim "Housing" stellt der Dienstleister lediglich Rechenzentrumsraum, Klimatechnik und ausfallsichere Stromversorgung zur Verfügung, nimmt jedoch keinerlei Wartungsarbeiten an Hard- oder Software vor. Hosting hingegen kann qualitativ von einfachen Wartungsarbeiten bis hin zu einer umfassenden Auftragsdatenverarbeitung gehen. Um den datenschutzrechtlichen Anforderungen gerecht zu werden und die physikalische Sicherheit sowie die Ausfallsicherheit zu gewährleisten, sollten folgende Maßnahmen bei der Beauftragung externer Dienstleister umgesetzt werden:

- vertragliche Ausgestaltung der technisch-organisatorischen Teilung der Zuständigkeit (siehe auch Kapitel 5.7.9),
- umfassende Regelung organisatorischer Fragen des Rechenzentrumsbetriebs (Fragen wie "Gibt es Arbeitsanweisungen zum Rechenzentrumsbetrieb?", "Wer hat Zugang zum Rechenzentrum?" und "Gibt es eine Rund-um-die-Uhr-Überwachung?" sollten geklärt sein),
- gestaffelte Service-Leistungen vom Betrieb zu normalen Bürozeiten bis hin zu einer umfassenden 7x24 Stunden-Versorgung,
- Zutrittsregelung nach dem Vier-Augen-Prinzip (Zugang für Personal des Dienstleisters nur gemeinsam mit einem Mitarbeiter des Anbieters),
- Server nicht in einem gemeinsam mit anderen Anbietern genutzten Rechenzentrumsraum, sondern in einem gesondert gesicherten und abgeschlossenen Bereich ("Käfig") aufstellen,
- möglichst wenig technische Ausstattung gemeinsam mit anderen Kunden nutzen (z. B. getrennte virtuelle LANs, unterschiedliche Router oder Loadsharer),
- Installation eines Firewallsystems beim Dienstleister zum Schutz des Servers und somit des Angebots,
- ausfallsichere Stromversorgung und Klimatechnik,
- angemessener Brandschutz,
- redundante Carrier-Anbindung,
- wirksame technische Absicherung des Zugangs zum Rechenzentrumsgebäude,
- sicherer Transport des Angebotes zum Dienstleister (beispielsweise Einspielen der Inhalte beim Servicedienstleister vor Ort durch Behördenmitarbeiter oder Fernadministration über einen entsprechenden Netzzugang mit sicherer Verschlüsselung, etwa mit ssh),
- regelmäßige Prüfung der Integrität des Angebotes
  - durch regelmäßige manuelle Kontrolle oder
  - durch automatisierte Kontrolle der Inhalte, beispielsweise durch Checksummenprüfung (siehe dazu auch eGovernment-Handbuch, Modul „Sicherer Internet-Auftritt im eGovernment“, Abschnitt 2.4).

Das Angebot sollte nicht in der Form des Webhosting bei einem so genannten Presence-Provider untergebracht werden, da sich bei dieser Dienstleistungsform in der Regel mehrere Anbieter dieselbe Hardwareplattform teilen, also mehrere Webserver auf dem selben Rechner laufen. Sämtliche Sicherheitsmaßnahmen können ausschließlich durch den Dienstleister wahrgenommen werden. Im Allgemeinen ist es bei dieser Dienstleistungsform nicht möglich, den "eigenen" virtuellen Server durch z.B. eine separate Firewall zu schützen.

<u>eGovernment-Server in der Behörde ohne Verbindung zum Hausnetz</u>
Grundsätzlich ergeben sich bei einer Unterbringung des Servers in den Räumlichkeiten der Behörde die gleichen Anforderungen an die physikalische Sicherheit des Servers wie an jeden anderen in der Behörde betriebenen Server. Zugangssicherung, Stromversorgung, Klimatechnik, Feuerschutz usw. müssen gewährleistet sein. Zu berücksichtigen ist dabei, dass das Webangebot wie bei einem externen Dienstleister meist rund um die Uhr zur Verfügung stehen soll. Obwohl in der Regel abends oder am Wochenende keine Wartung stattfindet, müssen für den Fall eines Angriffs auf

den Server wirkungsvolle und angemessene technische und organisatorische Maßnahmen vorgesehen werden. Auch wenn das Webangebot vollständig vom Hausnetz der Behörde getrennt ist, sollte der Webserver durch ein Firewallsystem im 7x24-Stunden-Betrieb geschützt werden, um die Integrität des eGovernment-Angebots sicherzustellen. Darüber hinaus müssen beispielsweise für den Fall eines ernsthaften Angriffs auf das Angebot Eskalationsmaßnahmen bis hin zum (zeitweiligen) Abschalten des Angebots bzw. der physikalischen Trennung vom Internet eingeleitet werden. Im Eskalationsplan (siehe auch Abschnitt 6.2.2) ist festzulegen, wer informiert wird, wer das Gefahrenpotential des Angriffs beurteilt und welche Maßnahmen eingeleitet werden, um die Integrität der Server zu gewährleisten.

eGovernment-Server in der Behörde mit Verbindung zum Hausnetz

Ist der eGovernment-Server in den Räumlichkeiten der Behörde untergebracht und mit dem Hausnetz verbunden, so ergeben sich zwei zusätzliche Bedrohungsszenarien:

- Ein Angriff auf das Angebot kann nicht nur aus dem Internet, sondern auch aus dem Behördennetz erfolgen.
- Wird die Firewall, die das Angebot schützt, bei einem Angriff überwunden, so erstreckt sich die Bedrohung auf das gesamte Behördennetz.

Der Integrität des Firewallsystems kommt in diesem Szenario eine nochmals erhöhte Bedeutung zu. Deshalb sollten Lösungen gewählt werden, die nicht nur das Web-Angebot der Behörde in einer demilitarisierten Zone (DMZ) schützen, sondern darüber hinaus auch die Integrität des Behördennetzes gegenüber dem Internet gewährleisten. Die Firewall hat in diesem Fall nicht nur den Verkehr mit dem Angebots-Server in der DMZ, sondern auch den möglichen Verkehr mit dem Behörden-LAN (falls die Mitarbeiter über Internetzugang verfügen) zu überwachen. Sinnvoll könnte hier ein mehrstufiges Firewallsystem sein, bei dem sich ein zusätzlicher Schutz beispielsweise durch ein Transfernetz und/oder weitere kaskadierte Firewalls ergibt. Solche Konstruktionen führen in der Regel zu einem weiteren Zeitvorteil für den Ablauf des Eskalationsplanes, da die Überwindung eines Transfernetzes und einer weiteren Firewall zusätzliche Zeit benötigt. Es besteht dabei die Möglichkeit, Kommunikation nur über Proxy-Server kontrolliert durch die Firewall zuzulassen oder Internetdienste über einen Terminalserver (remote display system, z. B. VNC) auf den einzelnen PCs des Hausnetzes lediglich graphisch darzustellen.
Ein mehrstufiges Firewallsystem bietet zudem den Vorteil, dass potentielle Angriffe aus einer bereits erfolgreich penetrierten DMZ oder dem Behördennetz auf das Webserver-Angebot erfasst werden können und sich ebenfalls ein Zeitvorteil für die Abwendung des Angriffs aus dieser Richtung ergibt.
Wartungsarbeiten an Firewallsystemen wie auch am Webangebot sollten nur über gesicherte Administrationszugänge (Verschlüsselung, Authentifizierung) aus dem Behördennetz, an den Systemen direkt vor Ort oder über einen Terminalserver erfolgen.
Bei den Planungen ist insbesondere zu berücksichtigen, dass zur Gewährleistung eines reibungslosen Rund-um-die-Uhr-Betriebs des Firewallsystems und seiner Komponenten sowie eines gesicherten Ablaufs des Eskalationsplanes ausreichend Personal vorzusehen und zu schulen ist und entsprechende Vertretungsregelungen erforderlich sind.

6.2 Organisatorische Werkzeuge

6.2.1 Sicherheitskonzept

Vor Einführung von eGovernment-Anwendungen ist eine systematische Analyse der mit der jeweiligen Anschlussart verbundenen Risiken und eine sorgfältige Auswahl geeigneter und angemessener technischer und organisatorischer Maßnahmen unumgänglich. Hierfür ist ein Sicherheitskonzept erforderlich, das in folgendem vierstufigen Verfahren erstellt werden sollte:

- Ermittlung des Kommunikationsbedarfs und der Schutzbedürftigkeit,
- Bedrohungsanalyse,
- Risikoanalyse,
- Auswahl konkreter Maßnahmen.

Der Aufwand bei der Erstellung von Sicherheitskonzepten hängt maßgeblich vom Schutzbedarf der zu verarbeitenden Daten ab. Sowohl die Datenschutzbeauftragten des Bundes und der Länder als auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI – www.bsi.bund.de) stellen Hinweise zur Schutzbedarfsfeststellung zur Verfügung. Die Auswahl einzelner Maßnahmen sollte in Abhängigkeit von dem festgestellten Schutzbedarf erfolgen. Sollte nach der abschließenden Auswahl der Maßnahmen die Risikoanalyse ein nicht zu vertretendes Restrisiko ergeben, muss auf einen Anschluss des internen Netzes an das Internet verzichtet werden. Der Zugriff auf eGovernment-Angebote kann in diesem Fall nur über solche Systeme erfolgen, die nicht mit dem Verwaltungsnetz verbunden sind. Weitergehende Hinweise zur Internetnutzung durch öffentliche Stellen bietet die Broschüre "Vom Bürgerbüro zum Internet" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Orientierungshilfe Internet des Arbeitskreises „Technik“.

Ein Sicherheitskonzept ist auch für den Fall erforderlich, dass das eGovernment-Angebot einem externen Dienstleister überlassen wird. Da die tatsächliche Sicherheit des Internet-Auftritts dann weitgehend in der Hand des Dienstleisters und nicht unter der Kontrolle der Behörde liegt, müssen dem Dienstleister bei Vertragsabschluss im Sicherheitskonzept verbindliche und wirksame Auflagen beispielsweise für die sichere Konfiguration und den sicheren Betrieb des WWW-Servers gemacht werden.

6.2.2 Konzepte für den laufenden Betrieb

Datensicherungskonzept

In einem Sicherungskonzept ist die Art und Weise der Datensicherung festzulegen, sodass der IT-Betrieb nach einem Schadensereignis durch einen redundanten Datenbestand kurzfristig wiederaufgenommen werden kann, auch wenn Teile des operativen Datenbestandes verloren gegangen sind. In Abhängigkeit von Menge und Bedeutung der zu verarbeitenden Daten sowie vom möglichen Schaden bei Verlust dieser Daten sind folgende Festzulegungen für die Datensicherung zu treffen:

- Zeitintervall (z. B. täglich, wöchentlich, monatlich),
- Zeitpunkt (z. B. nachts, Freitagabend),

- Anzahl der aufzubewahrenden Generationen (z.B. bei täglicher Komplettsicherung Aufbewahrung der letzten sieben Sicherungen, außerdem die Freitagabend-Sicherungen der letzten zwei Monate),
- Umfang der zu sichernden Daten (z.B. bestimmte Partitionen oder Verzeichnisse),
- Speichermedien (Bänder, Kassetten, Disketten, Spiegelung auf 2. Platte),
- Zuständigkeit für die Durchführung (Administrator, Benutzer),
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien),
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung / gewählte Parameter, Beschriftung der Datenträger).

Regelungen für das Eintreten von Sicherheitsvorfällen

Sicherheitsvorfälle können zum Beispiel eintreten durch Angriffe auf Internet-Server als kriminelle Handlungen (z.B. Hacking), durch Sicherheitslücken in den eingesetzten Hard- oder Softwarekomponenten, durch Schadsoftware wie Viren, Würmer oder Trojanische Pferde sowie durch Fehlverhalten von Bürgern oder auch Beschäftigten der Behörde, das zu Datenverlust oder sicherheitskritischer Änderung von Systemparametern führt. Die möglichen Schäden bei einem Sicherheitsvorfall können sowohl die Vertraulichkeit oder Integrität von Daten als auch die Verfügbarkeit betreffen. Zur Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb sind Festlegungen zur erforderlichen und angemessenen Reaktion zu treffen. Bekannte sicherheitsrelevante Schwachstellen in den Betriebssystemen und der Serversoftware sind stets unverzüglich durch Updates (Patches) der Hersteller zu beheben. Es ist zu empfehlen, sich in die Mailinglisten des Computer Emergency Response Teams (CERT -) und die der Hersteller eintragen zu lassen.

6.2.3 Revisionskonzepte

Ein wesentlicher Faktor der Systemsicherheit ist eine konsequente Revision. Hierbei sind die in Protokollen gesammelten Daten durch entsprechend autorisierte Mitarbeiter auszuwerten. Unregelmäßigkeiten beim Betrieb der IT-Systeme oder systematische Angriffen auf den Internet-Rechner und seine Komponenten können so aufgedeckt werden.

Die Protokollierung sollte so erfolgen, dass sensitive Aktivitäten und vorab zu definierende Systemzustände für eine nachfolgende Kontrolle festgehalten werden. Unter anderem sollte Folgendes protokolliert werden:

- Systemgenerierung und Modifikation von Systemparametern,
- Einrichten von Benutzern,
- Erstellung von Rechteprofilen,
- Einspielen und Änderung von Anwendungssoftware,
- Änderungen an der Dateiorganisation,
- Durchführung von Datensicherungsmaßnahmen,
- sonstiger Aufruf von Administrations-Tools,
- Datenübermittlungen,
- Zugriffe auf aktive Systemkomponenten,

- falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen, insbesondere sicherheitskritische Zugriffe mit oder ohne Erfolg,
- Verteilung der Rechner-/Systemlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance,
- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können.

Revision beschränkt sich jedoch nicht auf die Kontrolle der Datenverarbeitungsvorgänge des eigenen IT-Systems. Werden Dienstleister mit der Verarbeitung personenbezogener Daten beauftragt, muss sich die Revision durch die Behörde auch auf deren IT-Systeme beziehen. Dabei ist insbesondere die Einhaltung der vertraglichen Regelungen zu prüfen.

6.2.4 Technische Ausgestaltung von Auftragsverhältnissen

Die technisch-organisatorischen Sicherungen sind in einem Sicherheitskonzept festzulegen (z.B. Verschlüsselung, pseudonymisierte Nutzung, automatisierte Löschung, Zugriffsbeschränkungen, getrennte Speichermedien). Besondere Bedeutung erlangen technische Regelungen bei Wartung und Fernwartung. Um die zusätzlichen Risiken soweit wie möglich zu begrenzen, ist eine Fernwartung nur zulässig, wenn die verantwortliche Stelle das Fernwartungsunternehmen schriftlich beauftragt (siehe hierzu Abschnitt 5.7.9).

- In dem Vertrag sind die erforderlichen technischen und organisatorischen Maßnahmen festzulegen. Das Sicherheitskonzept (vgl. Punkt 6.2.1) sollte Vertragsbestandteil sein.
- Die Arbeiten sind so zu gestalten, dass das beauftragte Unternehmen keine Möglichkeit hat, auf gespeicherte personenbezogene Daten zuzugreifen. Sollte in Ausnahmefällen doch einmal ein solcher Zugriff notwendig sein, so unterliegen diese Daten einer Zweckbindung, d.h. das Unternehmen darf diese Daten ausschließlich für die erforderlichen Arbeiten nutzen. Eine Weitergabe der durch den Zugriff auf die Daten erworbenen Kenntnisse an Dritte ist zu untersagen.
- Die Aufschaltung auf einen entfernten PC (Bildschirmübernahme) im Rahmen des Teleservice sollte nicht ohne Wissen und aktive Mitwirkung des Nutzers erfolgen können. Nur wenn der Benutzer dem Wunsch auf Bildschirmübernahme, etwa durch Anklicken eines entsprechenden Buttons, zustimmt, darf eine solche Übernahme möglich sein.
- Die Systemeinstellungen, die diese Mitwirkung des Nutzers garantieren, dürfen sich nicht unbemerkt deaktivieren lassen. Der Nutzer sollte über die mögliche Bildschirmübernahme und ihre Mitwirkungsmöglichkeiten unterrichtet sein und jederzeit die Möglichkeit haben, die Bildschirmübernahme abzubrechen. Um nachträgliche Überprüfungen zu ermöglichen, sollten die Teleservice-Aktivitäten in angemessenem Umfang protokolliert werden. Auch die übrigen Formen des Teleservice sollten zuvor angemeldet und angemessen protokolliert werden. Ferner sind die Zugriffsmöglichkeiten des Service-Personals und der zum Service verwendeten Benutzerkennungen so weit wie möglich zu beschränken.

- Wird zur Abwicklung des Auftrags das lokale Netz des Auftraggebers mit einem Netz oder mehreren Netzen des Auftragnehmers gekoppelt, so sind diese Netzkoppelungen so zu gestalten, dass der Auftragnehmer nur dann auf einzelne Computer, Daten oder Dienste im Netz des Auftraggebers zugreifen kann, wenn dies zur Erledigung seiner vertraglichen Aufgaben erforderlich ist. Außerdem muss ausgeschlossen sein, dass das Netz des Auftragnehmers zum Einfallstor wird, über das Dritte das Netz des Auftraggebers angreifen können.
- Vielfach benötigt der Auftragnehmer umfassende Zugriffsberechtigungen (Administrationsberechtigungen) für die von ihm betreuten Systeme. Sind auf diesen Systemen auch personenbezogene oder andere schutzbedürftige Daten gespeichert, die der Auftragnehmer nicht zur Erfüllung seiner Administrationsaufgaben benötigt, so sind Schutzmaßnahmen zu ergreifen, die verhindern, dass Mitarbeiter des Auftragnehmers unberechtigt darauf zugreifen. Als Schutzmaßnahmen kommen dabei insbesondere die Protokollierung der Aktivitäten des Auftragnehmers und die Verschlüsselung der schutzbedürftigen Daten in Frage.
- Da Protokolldaten ihrerseits vielfach personenbezogen sind, ist darauf zu achten, dass nicht mehr Daten erfasst und aufbewahrt werden, als für die vorgesehene Auswertung relevant sind. Benötigt wird somit ein Konzept, aus dem hervorgeht, wann welche Auswertungen durchzuführen sind und welche Protokolldaten dafür benötigt werden. Da die Protokolldaten häufig sehr umfangreich sind, ist deren manuelle Auswertung häufig nicht praktikabel. Entscheidend ist daher, dass die Protokolldaten auch automatisiert ausgewertet werden können. Dabei sollten regelmäßig wiederkehrende Auswertungen erfolgen. Ferner sollte beim Auftreten sicherheitsrelevanter Ereignisse umgehend ein Alarm ausgelöst werden. Zugriffsmöglichkeiten auf diese Protokolldaten sollte neben dem Auftragnehmer auch der Auftraggeber erhalten.
- Bei der Suche nach einem geeigneten Verschlüsselungsprodukt ist zu beachten, dass eine SSL-Verschlüsselung, die mitunter zum Schutz der über Internet übertragenen Daten vorgesehen ist, keinen Schutz für die auf einem Server abgelegten Daten bietet, die z. B. mit Hilfe eines Web-Formulares erhoben wurden.

6.2.5 Nutzungsbedingungen für den Anwender

Der rechtliche Rahmen für die Inanspruchnahme von eGovernment-Diensten ist durch konkrete Nutzungsbedingungen zu regeln. Festzulegen sind:

- spezifische Voraussetzungen für die Inanspruchnahme und die Mitwirkungspflichten der Bürger (in Abhängigkeit vom Umfang des Online-Angebots, z.B. nur allgemeine Informationen, elektronische Abwicklung von Anträgen),
- gegebenenfalls Abgrenzung des Angebots der Verwaltung von dem Angebot anderer Behörden oder privater Rechtsträger,
- Regelungen zur rechtlichen Wirkung der elektronischen Willenserklärungen und der elektronischen Rechtsakte der Verwaltung,
- Voraussetzungen, unter denen elektronische Erklärungen schriftlichen Erklärungen gleichgestellt sind,

- Vorgaben zum Umgang mit der technischen Sicherheitsinfrastruktur überlassener Zugangssoftware,
- Regelungen zur Haftung bei mangelnder Verfügbarkeit der Dienste und für Verweise auf fremde Webseiten (Hyperlinks),
- Hinweise zur Verteilung des Fälschungs-, Übermittlungs- und Missbrauchsrisikos (Unter welchen Voraussetzungen hat der Bürger die Folgen einer fehlerhaften Übermittlung zu tragen und welche alternativen Zugangsmöglichkeiten kann er in Anspruch nehmen).

Die Nutzungsbedingungen sollten in das Online-Angebot der Verwaltung integriert sein, über einen deutlichen Hinweis auf der Angebotsseite leicht erreichbar sein, für den Bürger speicher- und auch ausdruckbar sein, klar strukturiert und leicht lesbar sein und an jeder Stelle des Dialogs durch einen deutlich gekennzeichneten Link aufrufbar sein. Darüber hinaus sollten die Nutzungsbedingungen Hinweise zu den Zahlungsmodalitäten enthalten. Insbesondere folgende Informationen sollten erfolgen:

- Zahlungswege und –bedingungen (auch zum nicht elektronischen Weg),
- Zeitpunkt des Zahlungsvorganges bei Einzugsermächtigung oder einer elektronischen Zahlung,
- Datensicherheit bei elektronischen Zahlungsverfahren und elektronischen Einzugsermächtigungen.

Erforderliche Zustimmungen müssen eine explizite Aktion des Nutzers erkennen lassen (Bestätigungsbutton, ggf. unter Hinzufügung des Passwortes o. Ä.), die zu protokollieren ist.

6.2.6 Beteiligung der Personalvertretung und des behördlichen Datenschutzbeauftragten

Durch die Möglichkeiten der Inhaltskontrolle und Protokollierung in eGovernment-Projekten können die einbezogenen Beschäftigten einer Verwaltung prinzipiell überwacht und ihre Leistung und ihr Verhalten kontrolliert werden. Deshalb ist es unerlässlich, eine Dienstvereinbarung mit der gewählten Personalvertretung abzuschließen, in der geregelt ist, was protokolliert wird, zu welchem Zweck Protokolldaten verwendet werden, wer Protokolle auswerten darf und wie lange Protokolle aufbewahrt werden.

Soweit die Protokollierungen der Aufrechterhaltung der Datensicherheit dient, ist festzuhalten, dass diese in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze unterliegen.

Der behördliche Datenschutzbeauftragten (bDSB) soll dazu beitragen, dass seine Behörde den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Der bDSB

- hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen,
- ist vor Einführung der entsprechenden IT-Verfahren u. a. durch Durchführung und Überprüfung des Ergebnisses der Vorabkontrolle nach den Regelungen des BDSG bzw. der entsprechenden Landesgesetze zu beteiligen,
- ist weiterhin zu beteiligen bei der Erstellung von Dienstanweisungen über getroffene bzw. zu treffende Datensicherungsmaßnahmen, bei Maßnahmen zum technisch-organisatorischen Datenschutz, bei der Auswertung von Protokollda-

teien, bei Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsverlangen und bei Bürgerbeschwerden mit Datenschutz-Bezug.

6.2.7 Personelle Maßnahmen

In eGovernment-Projekten sind frühzeitig Verantwortungsbereiche und Befugnisse für Anbieter und Anwender schriftlich festzugelegen. Es ist ein Rollen- und Zugriffsrechtekonzept zu erstellen, das regelt, welche Personen im Rahmen ihrer jeweiligen Funktion (Anwendungsentwickler, Systemadministrator, Anwenderbetreuer, Sachbearbeiter, Revisor, bDSB) welche IT-Anwendungen und welche Daten nutzen dürfen. Dabei dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Alle am eGovernment-Projekt beteiligten Personen sind vor der Aufnahme des Wirkbetriebes intensiv zu schulen. In größeren Behörden bzw. Unternehmen kann es sinnvoll sein, eine zentrale Stelle (User-Help-Desk) mit der Betreuung der IT-Benutzer zu beauftragen und diese allen Mitarbeitern bekannt zu geben. Diese Maßnahme kann sich insbesondere im Hinblick auf die Unterstützung der Bürger, die mit der Verwaltung kommunizieren, als sinnvoll und praktikabel erweisen.

6.3 Selbstdatenschutz

Neben den Maßnahmen, die der eGovernment-Anbieter trifft, hat der Nutzer von eGovernment-Angeboten die Möglichkeit, sich selbst durch geeignete Maßnahmen und Verhaltensweisen zu schützen.

Unterrichtung

Zu den wichtigsten Voraussetzungen für erfolgreichen Datenschutz gehört das Bewusstsein der Nutzer über Gefährdungen und Risiken. Selbstdatenschutz beginnt deshalb mit Information und Sensibilisierung. Eine wichtige Informationsquelle ist beispielsweise das so genannte Virtuelle Datenschutzbüro (http://www.datenschutz.de). Datenschützer aus verschiedenen Ländern stellen über das Internet in diesem Rahmen ein umfangreiches Informationsangebot zur Verfügung.

In zunehmendem Maße informieren eGovernment-Anbieter über den eigenen Umgang mit personenbezogenen Daten in so genannten Privacy Policies. Anwender sollten diese Möglichkeit nutzen, um sich vor der Inanspruchnahme einer elektronischen Dienstleistung über das Datenschutzniveau des Anbieters zu informieren.

Die Anbieter von eGovernment-Leistungen in Form eines Tele- oder Mediendiesntes sind zu einer solchen Unterrichtung nach § 4 Abs. 1 TDDSG und § 18 Abs. 1 MDStV verpflichtet.

Eine gute Möglichkeit, sich über Transparenz und Selbstbestimmungsmöglichkeiten bei jeder Kommunikation zu informieren, ist das Verfahren P3P (Platform for Privacy Preferences). Es steht für einen Internet-Standard des World Wide Web Consortiums (W3C), bei dem der Nutzer eine Kontrolle über seine Daten erhält, indem er zustimmen oder untersagen kann, dass seine Daten übermittelt werden. Dafür legt er fest, welche personenbezogenen Daten er zu welchem Zweck hergeben möchte. Der Anbieter wiederum definiert, welche Daten er benötigt und wie er sie verwenden will. Nur

wenn diese beiden Anforderungen von Nutzer und Anbieter im Einklang stehen, werden die Daten übermittelt.

Unbeobachtete Inanspruchnahme von eGovernment-Angeboten
Um dem Nutzer die vom Gesetzgeber geforderte Inanspruchnahme und Bezahlung von Tele- und Mediendiensten anonym oder unter Pseudonym zu ermöglichen (§ 4 Abs. 1 TDDSG/ § 13 MDStV), sollten u. a. Bezahlfunktionen so gestaltet werden, dass sie nicht zu einer Identifikation der Betroffenen führen, wenn diese auf Grund des elektronischen Verfahrens nicht ohnehin schon bekannt sind. Im Rahmen des Projektes „AN.ON“ (starke Unbeobachtbarkeit und Anonymität im Internet) wird der vertrauenswürdige Anonymisierungsdienst JAP (www.anon-online.de) gemeinsam von der TU Dresden, der FU Berlin und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein betrieben. JAP ermöglicht Internetnutzern das anonyme Surfen, ist somit ein wichtiges Werkzeug zum Selbstdatenschutz und unterstützt zudem die o. g. Forderung des Gesetzgebers.
Selbst bei Angeboten, bei denen es sinnvoll oder gar erforderlich ist, dass sich Nutzer und Anbieter elektronischer Dienstleistungen kennen, muss nicht zwangsläufig „der Rest“ der Internetnutzer von der Kommunikation zwischen beiden erfahren. Zwar kann ein einzelner Internetnutzer gegenüber einem Beobachter nicht anonym sein, in einer Gruppe von Nutzern kann die Forderung nach Unbeobachtbarkeit jedoch realisiert werden. Zu diesem Zweck werden die Anfragen der Gruppe von Nutzern nicht direkt zum Webserver geschickt, sondern nach dem Prinzip der so genannten Mixe über mehrere vertrauenswürdige Zwischenstationen zum Ziel geleitet. Diese Zwischenstationen wirken jeweils wie ein Proxy (zu deutsch Stellvertreter), der die gewünschte Seite anstelle des Nutzers abruft. JAP stellt neben einer ganzen Reihe derartiger Stellvertreter auch eine einfach zu bedienende Software bereit, mit der eGovernment-Anwender dieses wirksame Werkzeug zum Selbstdatenschutz bedienen können.

Verschlüsselungsangebote
Eine Maßnahme, mit der Bürgerinnen und Bürger sich bei der Nutzung von eGovernment-Angeboten schützen können, ist der Einsatz moderner kryptographischer Verfahren. Sie ermöglichen die Sicherstellung der Vertraulichkeit der Daten durch Verschlüsselung sowie den Nachweis der Integrität der Daten und der Überprüfung ihres Urhebers durch eine elektronische Signatur. Schon heute kann mit marktgängigen Softwareprodukten bei einem breiten Anwenderkreis eine sichere Kommunikation realisiert werden. Viele Produkte basieren beispielsweise auf der ISIS-MTT-Spezifikation, welche die technischen Rahmenbedingen auf Grundlage international anerkannter Internet-Standards regelt.
In zunehmendem Maße werden Internet-Angebote verschlüsselt bereitgestellt (http://www.netscape.com/tech/security/ssl/howitworks.html). So ermöglicht zum Beispiel SSL (Secure Socket Layer) die Absicherung der Kommunikationsbeziehung zwischen Nutzer-PC und Server des Diensteanbieters, indem es die Web-Seite durch digitale Zertifikate authentifiziert und die Kommunikation verschlüsselt abwickelt. Der Nutzer erkennt die Verwendung von SSL durch den Protokollzusatz HTTPS im Adressfenster des Browsers oder durch das Symbol eines geschlossenen Vorhängeschlosses in der Statuszeile des Browsers.

Das wohl am weitesten verbreitet Programm zur Verschlüsselung von eMails ist Pretty Good Privacy (PGP). PGP steht für viele verschiedene Systemplattformen zur Verfügung und kann für Privatanwender kostenfrei aus dem Internet heruntergeladen werden (z. B. ftp://ftp.de.pgpi.com/pub/pgp). Viele öffentliche Stellen bieten Bürgern eine verschlüsselte elektronische Kommunikation auf der Basis von PGP an, beispielsweise nahezu alle Datenschutzbeauftragten des Bundes und der Länder.
Als akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz stehen inzwischen 15 Anbieter zur Verfügung, die auf der Homepage der Regulierungsbehörde für Telekommunikation und Post (www.regtp.de) aufgelistet sind. Sie bieten signaturgesetzkonforme Signaturverfahren an, die nicht nur die Funktion der Signatur, sondern immer auch die Funktionen der Verschlüsselung und der Authentifikation bieten. Mit diesen Signaturen kann auch die gesetzliche Schriftform erfüllt werden.
Selbstdatenschutz bedeutet in diesem Zusammenhang, die angebotenen Verschlüsselungsmöglichkeiten ganz bewusst zu nutzen und digitale Zertifikate sorgfältig zu prüfen.

Sicherheitsmaßnahmen, die der Nutzer selbst aktivieren kann
Der Benutzer kann sich durch unterschiedliche technische Sicherheitsmaßnahmen gegen einige der vorhandenen Gefährdungen selbst schützen:

- Ausführen von aktiven Inhalten abschalten
  Diese Maßnahme bietet einen wirksamen Schutz gegen die Gefährdungen durch aktive Inhalte (Java-Applets, Javascript und ActiveX-Objekte). Aufgrund der Vielzahl von Software-Schwachstellen in den Browsern empfehlen inzwischen sogar die Browser-Hersteller, bei der Nutzung von aktiven Inhalten Vorsicht walten zu lassen.
- Signaturprüfungen aktiver Inhalte
  Mitunter kann jedoch aus bestimmten Gründen nicht auf die Nutzung aktiver Inhalte verzichtet werden. Für diesen Fall sollten Java-Applets, Javascript und ActiveX-Objekte mit einer elektronischen Signatur versehen sein. Diese Signatur dient dazu, die Integrität und Authentizität des jeweiligen aktiven Inhalts zu schützen. Der Benutzer sollte sich über seinen Browser anzeigen lassen, von wem der aktive Inhalt bereitgestellt und ob er unmanipuliert übertragen wurde.
- Schutz gegen Cookies
  Die standardmäßig verwendeten Browser bieten ein abgestuftes System zum Umgang mit Cookies. Der sicherste Schutz vor Cookies wird erreicht, indem das Speichern von Cookies auf der eigenen Festplatte durch die entsprechende Einstellung generell verboten wird. Das andere Extrem wäre die vollständige Freigabe für alle anfallenden Cookies. Da Cookies zur Überwachung des Nutzerverhaltens missbraucht werden können, sollten Anwender jedoch einen möglichst restriktiven Umgang mit Cookies auswählen. Insbesondere gegen die Erstellung von Nutzerprofilen mithilfe von Cookies existieren eine Reihe von Tools. So filtert das Produkt WebWasher EE der webwasher.com AG (http://www.webwasher.com) Cookies aus dem Datenstrom, der von einem Webserver zum Clientrechner des Nutzers verschickt wird. Der CookieCooker (**http://cookie.inf.tu-dresden.de**) verwaltet von Webservern gesetzte Cookies so, dass die unter diesen Cookies gespeicherten Nutzungsprofile möglichst

stark verfälscht werden und damit keine integeren Datensammlungen über die Webnutzung angelegt werden können.

- Sonstige Browsereinstellungen
  Über obige Optionen hinaus bieten die gängigen Browser unterschiedliche Konfigurationsmöglichkeiten für die Ausführung und die Zugriffsmöglichkeiten aktiver Inhalte. Beispielsweise kann im Internet-Explorer das Verhalten gegenüber ActiveX-Objekten detailliert eingestellt werden.

Anti-Viren-Software
Eine der wichtigsten Maßnahmen zum Selbstschutz ist die Installation von Anti-Viren-Software. Diese Produkte schützen insbesondere vor bereits bekannten Schadprogrammen, die zuverlässig identifiziert werden können. Allerdings muss die Datenbasis des Programms durch regelmäßige Updates ständig auf dem neuesten Stand gehalten werden. Inzwischen gibt es eine Reihe von Viren-Scannern, die auch aus dem Internet heruntergeladene aktive Inhalte (beispielsweise ActiveX-Objekte) nach Viren, Makroviren und Trojanischen Pferden durchsuchen können.

Personal Firewalls
Die eGovernment-Anbieter schützen ihre eigene Infrastruktur gegen Angriffe aus dem Internet in der Regel durch aufwändige Firewallinstallationen. Einerseits wären solche Schutzmaßnahmen für private eGovernment-Nutzer sicher überzogen, andererseits wären Anwender in den meisten Fällen ohnehin weder personell noch finanziell in der Lage, derartige Vorkehrungen zum Schutz des eigenen PC zu treffen. Eine sinnvolle Alternative zum Schutz des Nutzer-PC sind jedoch so genannte Personal-Firewalls. Diese Software wird auf dem Nutzer-PC (Notebook oder Desktop) installiert und schützt ihn vor Zugriffen aus dem Internet und vor Bedrohungen, die im Rahmen der erlaubten Kommunikation durch mitgesendete bösartige Inhalte entstehen können. Einige Personal-Firewalls sind bereits in der Lage, die Ausführung aktiver Inhalte zu kontrollieren und unautorisierte Verbindungsaufbauten anzuzeigen und zu unterbinden. Ihr Einsatz ist insbesondere in Verbindung mit einem Anti-Viren-Produkt sinnvoll.

7 Beispielhafte Lösungen für einzelne eGovernment-Anwendungen

Im Folgenden werden Lösungsansätze für eGovernment-Anwendungen dargestellt. Die aufgeführten Anwendungen sind von der jeweils zuständigen Datenschutzaufsicht zusammengestellt und auf ihre Vereinbarkeit mit den rechtlichen und technisch-organisatorischen Datenschutzleitplanken geprüft worden. Sie sind insoweit als Grundschutz zu verstehen, der im Sinne einer verbesserten datenschutzrechtlichen Gestaltung im Einzelfall ggf. weiter optimiert werden kann. Da die rechtlichen Regelungen in den einzelnen Ländern nicht immer identisch sind, sollten Sie, wenn Sie vergleichbare Anwendungen planen, unbedingt Kontakt mit der für Sie zuständigen Datenschutzaufsichtsbehörde aufnehmen, damit geklärt werden kann, welche datenschutzrechtlichen Anforderungen im konkreten Einzelfall zu erfüllen sind.
Die Auswahl hat sich an dem Ziel orientiert, für möglichst viele und typische Bereiche des eGovernment Referenzanwendungen zu benennen und dadurch den Zugang zum eGovernment gerade auch für solche Träger zu erleichtern, denen eigene Ent-

wicklungskapazitäten oder –ressourcen nur in einem beschränkten Umfang zur Verfügung stehen. Beispielhafte Lösungen können sowohl in der Entwicklung und dem Einsatz datenschutzgerechter fachübergreifender Anwendungen als auch in der datenschutzgerechten Ausgestaltung von Fachanwendungen liegen. Um die praktische Umsetzung zu belegen, sind die Anwendungen mit Projektbeispielen verbunden worden. Es ist jedoch nicht beabsichtigt, anderen als den hier erwähnten Projekten ihre datenschutzgerechte Gestaltung abzusprechen.

7.1 Fachübergreifende Anwendungen

Der Einsatz von Basismodulen ist in vielen Fällen Voraussetzung für die elektronische Abwicklung von Fachanwendungen im Rahmen des eGovernment. Basismodule beinhalten Grundfunktionalitäten, die „quer“ zu den jeweiligen Fachanwendungen die elektronische Abwicklung von Verwaltungsdienstleistungen und den damit verbundenen Verwaltungsvorgängen ermöglichen oder erleichtern. Je nach den spezifischen Anforderungen der jeweiligen Fachanwendung müssen Basisanwendungen bei Bedarf mit den darin enthaltenen Werkzeugen an individuelle Anforderungen angepasst werden. Ergänzend wird in diesem Zusammenhang auf die Hinweise und Handlungsempfehlungen im Kapitel 5.7.1 bis 5.7.10 verwiesen.

7.1.1 Akteneinsicht

Die Stadt Rathenow hat im Rahmen des Städtewettbewerbs Media@komm einen Förderpreis für das Projekt „Elektronische Akteneinsicht“ erhalten. Seitdem setzt die Stadt das Projekt in enger Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sowie dem Landesbetrieb für Datenverarbeitung und Statistik schrittweise um. Ziel des Projektes ist es, den nach dem brandenburgischen Akteneinsichts- und Informationszugangsgesetz (AIG) grundsätzlich voraussetzungslosen Zugang zu den von der Verwaltung vorgehaltenen Informationen auch elektronisch über das Internet zu ermöglichen. Einerseits wird die Stadt das so genannte City-Informationssystem auf einem Webserver zum Abruf über das Internet bereitstellen. Dort werden Dokumente vorgehalten, zu denen ein voraussetzungsloser Zugang besteht und die nach unterschiedlichen Rechtsvorschriften ohnehin öffentlich gemacht werden können oder müssen, wie z. B. Satzungen, Unterlagen aus öffentlichen Sitzungen der Stadtverordnetenversammlung usw. Insoweit besteht kein wesentlicher Unterschied zu vielen anderen Kommunen. Darüber hinaus wird die Stadt Rathenow aber auch Akten und Dokumente aus dem gewöhnlichen Verwaltungsvollzug für einen elektronischen Zugang bereitstellen. Zur Umsetzung des Projektes hat die Stadt zunächst ihren Aktenplan sowie das Dokumentenaufkommen analysiert, einen transparenten Aktenplan geschaffen und ein Dokumentenmanagement-System (DMS) ausgewählt. Derzeit wird das DMS sowie das elektronische Archivsystem zunächst für einige Ämter implementiert und die Internet-Schnittstelle entwickelt, bevor die elektronische Akte als Voraussetzung für eine elektronische Akteneinsicht zunächst in einer Pilotphase eingeführt wird. Will ein Bürger in eine elektronische Akte einsehen, wird er in der Regel zunächst per eMail bei der Stadt anfragen. Der zuständige Bearbeiter wird dann zunächst die relevanten Akten bzw. Dokumente identifizieren. Ist die Akte noch nicht in elektronischer Form vorhanden, ist ad hoc eine Digitalisierung der Dokumente möglich. Der Bearbeiter prüft dann, ob und in welchem Umfang die Dokumente für eine Akteneinsicht zur Verfügung stehen. Bestehen keine Geheimhaltungsgründe aus öffentlichem oder überwiegenden privatem Interesse nach §§ 4, 5 AIG, so werden die Dokumente ohne weiteres dem Anfragenden per eMail zur Verfügung gestellt. Ebenso wird verfahren, wenn die nicht ohne weiteres zugänglichen Teile entsprechend § 6 Abs. 2 AIG ausgesondert werden können. Eine Identifizierung des Anfragenden ist in diesem Falle nicht erforderlich und soll auch nicht erfolgen. Durch Vergabe eines eindeutigen Schlüssels für die Anfrage ist sichergestellt, dass nur der Anfragende die entsprechenden Dokumente erhält. Muss die Akteneinsicht abgelehnt werden oder ist der Inhalt nach §§ 4, 5 AIG geheim zu halten, erhält der Antragsteller eine entsprechende Nachricht. In diesen Fällen wird eine Identifizierung des Antragstellers mit qualifizierter elektronischer Signatur verlangt, weil die Ablehnung ein Verwaltungsakt ist und der Antragsteller dagegen Rechtsmittel einlegen kann. Enthalten die Dokumente personenbezogene Daten oder geheim zu haltende unternehmensbezogene Daten und soll die Zustimmung des Betroffenen eingeholt werden, ist ebenfalls eine Identifizierung des Antragstellers erforderlich. Durch ein Serverzertifikat, das durch den Landesbetrieb für Datenverarbeitung und Statistik bereitgestellt wird, wird sichergestellt, dass die übermittelten Dokumente von der Stadt Rathenow stammen.

Die elektronische Akteneinsicht in Rathenow wird einen bürgerfreundlichen und auch datenschutzgerechten elektronischen Zugang zu den in der Verwaltung vorgehaltenen Informationen realisieren.

Ansprechpartner:

Stadtverwaltung Rathenow
Berliner Str. 15
14712 Rathenow
Tel.: (03385) 596-0
Fax: (03385) 596-1044
Mail: poststelle@rathenow.brandenburg.de
Internet: www.rathenow.de

7.1.2 Archivierung

Das Forschungsprojekt „Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente (ArchiSig)“ hat über die Aufbewahrung einfacher elektronischer Dokumente hinaus ein Verfahren entwickelt, wie auch elektronisch signierte Dokumente langfristig aufbewahrt und zur Erhaltung ihres Beweiswerts bei Bedarf automatisiert neu signiert werden können.

Verfahrensbeschreibung

Die aufzubewahrenden signierten Dokumente werden bei der Aufnahme in das Archivsystem auf ihre Integrität und Authentizität überprüft. Die für eine langfristige Signatur- und Authentizitätsprüfung erforderlichen Verifikationsdaten (insb. Zertifikate und Gültigkeitsabfragen) werden beschafft. Die elektronischen Dokumente werden verschlüsselt auf Langfristspeichermedien gespeichert. Die Verifikationsdaten und die Signaturen der Dokumente und Zertifikate werden in einem getrennten System für die Signaturerneuerung gespeichert. Werden bestimmte Algorithmen und Parameter von der Regulierungsbehörde nicht mehr für die folgenden sechs Jahre als sicher prognostiziert, stößt das Verfahren automatisch eine Erneuerung der betroffenen Signaturen an. Diese erfolgt im Regelfall ohne Zugriff auf die elektronischen Dokumente. Vielmehr werden viele Signaturen zusammengefasst und jeweils mit einem Zeitstempel, der eine qualifizierte Signatur trägt, erneut signiert.

Datenverarbeitung

Für die Signaturerneuerung ist ein Zugriff auf die personenbezogenen Daten in den elektronischen Dokumenten im Regelfall nicht erforderlich. Dies wird erst dann notwendig, wenn die verwendeten Hashverfahren unsicher werden. Ein Zugriff auf die signierten Dokumente im Klartext ist jedoch auch hier nicht zwingend notwendig. Dies gilt zumindest dann, wenn sie nach der Signaturerstellung unter Einbeziehung aller Signaturen und gegebenenfalls aller erforderlichen Verifikationsdaten verschlüsselt und dann nochmals gehasht und signiert werden. Für die Signaturerneuerung sind dann nur noch die verschlüsselten Daten maßgeblich. Das auf dem Konzept der Hashwertbäume basierende Verfahren ermöglicht auch, für die langfristig aufbewahrten Dokumente einzelne Dokumentteile, Daten und Signaturen zu berichtigen, zu löschen und zu sperren, ohne dabei die Beweiskraft der anderen erneuerten Signaturen anzugreifen.

Datenschutzrechtliche Bewertung

Die langfristig aufbewahrten personenbezogenen Daten (in den Dokumenten und den Zertifikaten) können trotz der Notwendigkeit einer in Abständen erforderlichen Neusignierung durch Verschlüsselung geschützt werden. Die bei der Neusignierung zu verarbeitenden Signatur- und Hashwerte sind keine personenbezogenen Daten. Durch diese Verfahren können auch besonders schützenswerte Daten für die langfristige Aufbewahrung und Neusignierung an fremde Dienstleister übermittelt werden. Sie erlauben auch, die Rechte der Betroffenen auf Sperrung und Löschung umzusetzen, ohne die Beweisqualität der Signaturen zu gefährden.

Projektverantwortung

Konsortialführer:
PERGIS Systemhaus GmbH
Andreas Bess
Rheinuferstr. 9
67061 Ludwigshafen
eMail: Andreas.Bess@pergis.de.

Datenschutzrecht:
Stefanie Fischer-Dieskau
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel
Mönchebergstr. 21a
34109 Kassel
Telefon: 0561/804-3079
EMail: s.fischer-dieskau@uni-kassel.de

7.1.3 Call-Center in Niedersachsen

Die niedersächsische Staatskanzlei ist dem Vorbild von Unternehmen gefolgt und bedient sich zur Beantwortung von Bürgeranfragen eines so genannten Call-Centers, um so kundenorientiert und schnell Auskunft über Fragen an die Landesverwaltung geben zu können. Mit der technischen Abwicklung dieser Leistung ist das Informatikzentrum Niedersachsen (izn) betraut worden.
Das Call-Center liefert grundsätzlich allgemeine Informationen, ohne dabei personenbezogene Daten der anrufenden Bürgerinnen und Bürger zu erfragen. Bei weitergehenden Serviceleistungen (Versand von Informationsmaterial, Rückfragen im Fachressort, Weiterleitung der Anfrage an die zuständige Fachbehörde) werden bis zur endgültigen Beantwortung und Abwicklung der Anfrage die erforderlichen Kommunikationsdaten erhoben und temporär gespeichert. Der erforderliche Datensatz für die einzelnen Serviceleistungen wurde festgelegt und es wurden angemessene Schutzvorkehrungen gegen eine missbräuchliche Verwendung getroffen. Die anfragenden Bürgerinnen und Bürger werden unterrichtet, mit wem sie im Kontakt stehen. Dienstleistungen, bei denen Daten erhoben werden müssten, die besonderen Berufs- und Amtsgeheimnissen unterliegen, sind dem Call-Center nicht übertragen worden.

Datenschutzrechtliche Bewertung

Die Anrufer werden darauf hingewiesen, dass sie Kontakt mit einem Call-Center und nicht mit der Behörde selbst haben. Den Anrufern wird die Möglichkeit eingeräumt, von sich aus mit dem zuständigen Ansprechpartner bei der Behörde in Kontakt zu treten, indem der Name des zuständigen Bearbeiters sowie die dienstliche Anschrift und Telefonnummer genannt werden. Die Anrufer werden darüber informiert, welche Daten über sie beim Kontakt mit dem Call-Center verarbeitet werden. Sie werden darüber aufgeklärt, dass sie ihre datenschutzrechtlichen Betroffenenrechte (Auskunft über gespeicherte Daten, Berichtigung und/oder Löschung der Daten) jederzeit gegenüber der auftraggebenden Behörde geltend machen können.

Nach Abschluss des Probebetriebs wird ein Vertrag zwischen Staatskanzlei und Call-Center unter Zugrundelegung der Regelungen über die Datenverarbeitung im Auftrag abgeschlossen, der neben den Pflichten des Auftragnehmers auch die technischen und organisatorischen Maßnahmen zum Schutz der Daten festschreibt sowie die frühestmögliche Löschung der Daten im Call-Center sichert. Mit der Personalvertretung wird eine Dienstvereinbarung getroffen, die die Protokollierung und Kontrolle regelt.

Projektverantwortung

Bei der Umsetzung dieses Projekts arbeiten die Niedersächsische Staatskanzlei und das Informatikzentrum Niedersachsen zusammen.

Ansprechpartner

Niedersächsische Staatskanzlei– Zentralstelle IuK
Ministerialrat Jürgen Burdorf
Tel. 0511-120-6756; eMail: Juergen.burdorf@stk.niedersachsen.de

7.1.4 Governikus – Client- und Backendanwendungen

Basismodul für datenschutzgerechtes, sicheres und rechtsverbindliches eGovernment

Das von der bremen online services GmbH & Co. KG (www.bos-bremen.de) entwickelte Basismodul „Governikus“ erbringt alle Funktionen, die benötigt werden, damit die öffentliche Verwaltung und ihre Kunden datenschutzgerecht, sicher und rechtsverbindlich über das Internet kommunizieren können.
Die Intermediäre, wie hier Governikus in den Media@Komm-Projekten, haben nach der Projektbeschreibung (siehe www.osci.de) folgende Aufgaben:

- Empfang der SigG-konform signierten und verschlüsselten Formularinhalte in Form von OSCI-Nachrichten
- Entschlüsselung der Absender- und Empfängerzertifikate von OSCI-Nachrichten und Prüfung der Gültigkeit
- Generierung des elektronischen Laufzettels zur Protokollierung der Verbindungs- und Prüfinformationen
- Bereitstellung eines virtuellen Postfaches für den Empfang von Nachrichten
- Zielgerichtete Weiterleitung der OSCI-Nachrichten an den Empfänger, wobei Inhaltsdaten verschlüsselt übertragen werden
- Zielgerichtete Weiterleitung der OSCI-Nachrichten an den Empfänger, wobei Inhaltsdaten verschlüsselt übertragen werden

Zusätzlich können weitere Aufgaben abgewickelt werden, wie:

- Bereitstellung von Formularen auf einem Formularserver
- Zahlungsabwicklung
- Virtuelle Poststelle, z. B. Geschäftsstelle für Gerichte und Behörden

Mit Hilfe von Governikus können beliebige Fachanwendungen auf Client- und Backendseite effektiv integriert werden. Die Software bildet die technische Basis des eGovernment-Portals der Freien Hansestadt Bremen (www.bremer-online-service.de) und wird auch von anderen Ländern und Kommunen eingesetzt. Beispielhaft sei auf die in acht Bundesländern eingeführten Online-Mahnverfahren ProfiMahn (www.profimahn.de) und OptiMahn (www.optimahn.de) verwiesen (für weitere Referenzen siehe www.bos-bremen.de). Governikus ist die erste Implementierung des eGovernment-Standards OSCI (www.osci.de).

Beschreibung

Der typische Ablauf einer eGovernment-Transaktion auf Basis von Governikus lässt sich wie folgt beschreiben: Ein Bürger/Kunde der Verwaltung erzeugt ein elektronisches Dokument mittels eines Web-Formulars (HTML, PDF etc.) oder mittels einer beim Kunden vorhandenen Standardsoftware (MS-Office Produkt, Anwaltssoftware, Buchhaltungssoftware etc.). Über eine Schnittstelle wird das elektronische Dokument automatisch an den Governikus-Client übergeben. Der Governikus-Client ist eine signierte Java-Applikation, die aus dem Internet heruntergeladen werden kann. Er übernimmt das Signieren, Verschlüsseln und Versenden des elektronischen Dokuments. Governikus ist in der Lage, mit unterschiedlichen Signaturniveaus (akkreditiert, qualifiziert, fortgeschritten) und unterschiedlichen TrustCentern (TeleSec, Datev, D-Trust, TC-TrustCenter etc.) umzugehen. Das elektronische Dokument wird vom Governikus-

Client nach dem Signieren und Verschlüsseln nicht direkt an die zuständige Verwaltungsstelle, sondern zunächst an einen zentralen Kommunikationsserver (Governikus-Intermediär) übermittelt.
Der Governikus-Intermediär übernimmt für eine Mehrzahl von Verwaltungsstellen die Funktionen einer „virtuellen Poststelle“. Er wird in der Regel in der „Demilitarisierten Zone“ eines Rechenzentrums betrieben. Der Governikus-Intermediär speichert die eingehenden Nachrichten in das „virtuelle Postfach“ der zuständigen Verwaltungsstelle und führt zugleich automatisch alle erforderlichen Signatur- und Zertifikatsprüfungen durch. Die Prüfungen werden zusammen mit dem Zeitpunkt des Nachrichteneingangs in einem signierten Übermittlungsprotokoll dokumentiert, das sowohl dem Absender als auch dem Empfänger zu Nachweiszwecken zur Verfügung steht (Einschreiben-mit-Rückschein-Funktion). Die zuständige Verwaltungsstelle kann sich die in ihrem „virtuellen Postfach“ befindlichen Nachrichten dann jederzeit zu Weiterbearbeitung abholen. Hierfür verwendet sie ebenfalls einen Governikus-Client. Der Weg eines elektronischen Dokuments *von* der Verwaltung *zum* Bürger/Kunden verläuft in gleicher Weise. Neben den eben beschriebenen asynchronen Transaktionen ermöglicht Governikus auch die „Echtzeitkommunikation“ zwischen Client-Anwendungen und Fachverfahren der Verwaltung. Charakteristisch für dieses Szenario ist,

- dass der Kunde - nach erfolgter Authentisierung - bereits während der Erstellung des elektronischen Dokuments mit dem Fachverfahren der Verwaltung kommuniziert und
- dass das Fachverfahren den Vorgang während der Online-Session ohne Mitwirkung eines Mitarbeiters abschließend bearbeitet (Vgl. als Beispiel für ein solches Verfahren die Online-Ummeldung auf Basis von Governikus unter www.bremer-online-service.de).

Datenschutzrechtliche Bewertung:

Das **Basismodul** „Governikus“ wird den Anforderungen eines wirksamen Datenschutzes gerecht. Im Einzelnen gewährleistet die Software....

....die *Vertraulichkeit* personenbezogener Daten bei der Nachrichtenübermittlung durch den Einsatz starker Verschlüsselungsverfahren. Eingesetzt werden ausschließlich allgemein anerkannte Kryptoalgorithmen (Triple-DES, RSA).

....die *Zweckbindung* personenbezogener Daten durch eine strikte Trennung von Inhalts- und Transportdaten. Der als virtuelle Poststelle für verschiedene Organisationseinheiten fungierende Governikus-Intermediär ist nicht in der Lage, die Inhaltsdaten zu interpretieren, weil diese ausschließlich für den Endempfänger verschlüsselt sind.

....die *Integrität und Authentizität* personenbezogener Daten durch den skalierbaren Einsatz elektronischer Signaturen.

....die *Nichtabstreitbarkeit* der Übermittlung personenbezogener Daten durch die sichere Protokollierung des Nachrichteneingangs (Einschreiben-mit-Rückschein-Funktion).

Anmerkung:
Soweit die Daten verarbeitende Stelle (der Intermediär) über die eigentliche Vermittlung **weitere** Aufgaben erfüllt und dazu Adressdaten- und/oder Inhaltsdaten zur Kenntnis nimmt und ggf. sogar weiterverarbeitet, geht eine solche Datenverarbeitung über die Funktion eines Intermediärs hinaus und muss daher gesondert datenschutzrechtlich beurteilt werden.
Soweit z.B. für die automatisierte Erstellung von Bescheiden (z.B. die Erstellung von Parkausweisen) die Daten im Klartext verarbeitet werden, stellt dies eine Datenverarbeitung im Auftrag dar, die nach Weisung des Auftraggebers erfolgt.

Weiterhende Informationen finden Sie auch im Kapitel 7.3.2 (Umsetzung von Media@Komm im Bundesland Bremen).

Hersteller:
bremen online service GmbH & Co. KG
Am Fallturm 9
28359 Bremen
Tel. 0421-204950

info@bos-bremen.de

7.1.5 Mobiles Arbeiten in der Geschäftsstelle des Landesbeauftragten für den Datenschutz Niedersachsen (LfD)

In Wirtschaft und Verwaltung werden Versuche zum mobilen Arbeiten unternommen. Damit sollen berufliche Tätigkeiten außerhalb konventioneller Betriebsstätten unter Nutzung von Telekommunikation durchgeführt werden. Im Gegensatz zur klassischen Telearbeit wird bei mobilem Arbeiten besonderes Gewicht auf große räumliche Beweglichkeit gelegt. Für den Zugriff auf zentral vorgehaltene Informationen werden Informationen entweder via eMail über das Internet ausgetauscht oder ein Remote-Anschluss zu einer Workstation oder einem Server betrieben. Neu ist die Terminal-Server-Technik, sie ermöglicht den Fern-Zugang zu Daten und Ressourcen einer Organisation, ohne dass diese Daten den geschützten Bereich des lokalen Netzwerkes verlassen. Hierzu wird ein Server installiert, der intern als Proxy für den externen Nutzer fungiert. Die Steueranweisungen werden in Form von Tastatur und Maus-Eingaben des externen Nutzers vom Terminal-Server empfangen und die Bildschirm-Darstellung zum externen Nutzer gesendet. Die Übertragung dieser Informationen wird bereits protokollseitig verschlüsselt, sodass fremde Kenntnisnahme oder Manipulation praktisch ausgeschlossen werden kann. Für die Steuerung dieses Proxies werden auf externen Systemen sog. Clients verwendet, die für die Kommunikation mit dem Terminal-Server sorgen. Diese Clients stehen sowohl auf Thin-Clients (dumme Terminals) als auch als reine Softwarelösung für die unterschiedlichsten Systeme zur Verfügung. Abschließende Ergebnisse werden Mitte 2003 vorliegen.

Technische Lösung

- Terminalserver

Der Terminal Server ist eine im Windows 2000 Server integrierte Funktion, die es mehreren Benutzern erlaubt, sich gleichzeitig über ein Netzwerk an dem Server anzumelden und dessen Ressourcen zu nutzen. Dazu wird auf dem Arbeitsplatz-PC oder einem anderen geeigneten Endgerät in einem Fenster eine vollständige Benutzeroberfläche dargestellt. Tatsächlich befindet sich diese Benutzeroberfläche aber auf dem Terminalserver. Die Benutzer können die ihnen zur Verfügung gestellten Applikationen (z.B. MS Office, Outlook, Acrobat Reader) nutzen und im Rahmen der dienstlichen Notwendigkeit auf andere Ressourcen im Netzwerk zugreifen. Der Server ist mit zwei Netzwerkkarten ausgestattet. Mit einer Karte wird der Server in das lokale LAN eingebunden, mit der zweiten Karte wird ausschließlich die Verbindung zwischen dem Terminalserver und dem Telearbeitsplatz hergestellt.

- Citrix Metaframe XP

Das Citrix Metaframe XP Paket ist ein Aufsatzprodukt für den Terminal Server, das den Funktionsumfang erweitert. Neben einer vereinfachten Administration und einem umfangreicheren Monitoring bietet Metaframe vor allem ein alternatives Übertragungsprotokoll (ICA-Protokoll) an, das performanter als das RDP-Protokoll des Terminal Servers ist. Wichtig ist dabei die Möglichkeit der Leitungsverschlüsselung über 128 Bit SSL. Dadurch lässt sich die Übertragung der Daten zwischen dem Telearbeitsplatz und dem Terminalserver wirksam absichern.

- Thin Client

Der Thin Client dient dem Telearbeitenden als Terminal für den Terminalserver. Handelsübliche Geräte verfügen über die gängigen Schnittstellen zum Anschluss von

Tastatur, Maus, Monitor und anderen Peripheriegeräten. Im Gerät sind jedoch keine Laufwerke oder Festplatten eingebaut. Als Betriebssystem werden überwiegend Windows CE oder Linux eingesetzt. Der in diesem Projekt eingesetzte Thin Client der Fa. IGEL wird unter Windows CE betrieben.

- Die Datenübertragung

Der Thin Client stellt über einen ISDN-Router eine Wählverbindung zu einem Knotenpunkt des vom Informatikzentrum Niedersachsen betriebenen iznNet2000 her. Von dort wird die Verbindung mittels statischer Routeneinträge zum Router des LfD hergestellt. Hierfür ist die Bandbreite eines Standard ISDN-Anschlusses mit 64 kbps ausreichend. Die Verbindung wird über die Landesfirewall beim izn und die Firewall des LfD zwischen dem Thin Client und dem Terminalserver geschaltet. Vom Terminalserver werden die reinen Bildinformationen zur Darstellung des Desktops an den Thin Client übertragen, umgekehrt sind es die am Telearbeitsplatz ausgelösten Tastatur- und Mauseingaben. Alle Bild- und Tastaturströme werden verschlüsselt übertragen. Die eigentliche Datenverarbeitung findet im geschützten Serverbereich statt. Somit verlassen die Anwendungsdaten nicht die Dienststelle.

Datenschutzrechtliche Bewertung

Alle Systemfunktionalität (Mail, Datenbanken, zentrale Serverablagen, Internet, etc.), werden über die Firewall mit allen Sicherheitsanforderungen realisiert. Die Verschlüsselung der reinen Bilddaten sowie der Tastaturanschläge und Mausbewegungen schafft ein hohes Maß an Sicherheit auf dem Datentransportweg. Die Terminalserver-Lösung erfüllt damit alle Sicherheitsanforderungen.

Projektbetreiber:

Landesbeauftragter für den Datenschutz Niedersachsen
Brühlstr. 9
30169 Hannover
Ansprechpartner: Manfred Grabow
Telefon: 0511-120-4532
EMail: manfred.grabow@lfd.niedersachsen.de

7.2 Fachanwendungen

Aufbauend auf den Basismodule entstehen beim eGovernment zunehmend fachbezogene Anwendungen, die sowohl nach außen gerichtete Verwaltungsleistungen einbeziehen als auch die internen Verwaltungsvorgänge betreffen. Die Arbeitsgruppe will auch hier beispielhafte und datenschutzgerechte Lösungen darstellen, wobei möglichst viele Anwendungsfelder von eGovernment einbezogen werden sollen.

7.2.1 Abfallbehälter der Stadt Krefeld

Neben diversen anderen Online-Anträgen bietet die Stadt Krefeld auch die Möglichkeit, Abfallbehälter abschließend über das Internet zu bestellen.

Verfahrensbeschreibung:

Die Anwendung umfasst die Abfallbehälter für Restmüll, Biomüll und Papier. Für jeden dieser Behälter können wahlweise die Neuaufstellung, Abholung, Volumenvergrößerung oder Volumenreduzierung beantragt und die gewünschte Anzahl, Größe und Leerungshäufigkeit ausgewählt werden.

Datenverarbeitung:

Informationen und die dem Antrag zugrunde liegenden Rechtsgrundlagen sind ohne Angabe von persönlichen Daten für jede/n Interessierte/n erreichbar. Im Antrag werden nur solche Daten erhoben und gespeichert, die für den Einzelfall zutreffend und für das weitere Verfahren notwendig sind. Hierüber wird der Nutzer und die Nutzerin im Impressum und mit Aufruf des Formulars informiert. Die Eingabe aller Daten ist freiwillig. Unmittelbar nach der Speicherung wird das Antragsdokument automatisiert in eine andere Datenbank kopiert und in der Ursprungsdatenbank gelöscht. Der Weg des Dokumentes kann vom Internet aus nicht nachvollzogen werden. Die Antragsdatenbank ist darüber hinaus nicht über Hyperlinks zu erreichen. Ein Ausspionieren der eingegangenen Daten über das Internet ist damit faktisch ausgeschlossen. Eine Weitergabe von Daten an Dritte findet nicht statt. Die Speicherung richtet sich nach den bestehenden gesetzlichen Vorschriften. Anonymisierte Daten über die Nutzerinnen und Nutzer der Krefelder Internetpräsentation werden in Log-Dateien gespeichert. Durch die Verkürzung der IP-Adressen um die letzten drei Ziffern ist ein Rückschluss auf den einzelnen Nutzer und die Nutzerin ausgeschlossen. Die Log-Dateien werden ausschließlich für Zwecke der Datensicherheit und für statistische Zwecke erhoben und nach zwei Monaten gelöscht.

Datenschutzrechtliche Bewertung:

Das Verfahren entspricht den datenschutzrechtlichen Vorgaben. Die Eingaben werden verschlüsselt übermittelt. Dadurch sind sie vor der Kenntnisnahme Dritter und Verfälschung geschützt. Eingesetzt wird eine SSL-Verschlüsselung mit 128 Bit Verschlüsselungsstärke, die auch zukünftig weiter der fortschreitenden technischen Entwicklung angepasst werden wird. Der Zugriff auf den eingegangenen Online-Antrag und die darin enthaltenen personenbezogenen Daten ist ausschließlich dem/der zuständigen Bearbeiter/in des Fachbereichs/Fachamtes eingeräumt. Der Personenkreis, dem der Inhalt eines eingegangenen Onlineantrags bekannt wird, ist damit kleiner als der, der Kenntnis vom schriftlichen Posteingang erhält.

Projektbetreiber:

Oberbürgermeister der Stadt Krefeld
Konrad-Adenauer-Platz 17
47792 Krefeld
www.krefeld.de; stadtservice@krefeld.de

7.2.2 Anwohnerparkausweis der Städte Erlangen, Fürth und Nürnberg

Beim Verfahren ”Anwohnerparkausweis” im Rahmen des MEDIA@Komm-Projektes des Städteverbundes Nürnberg handelt es sich um eine Anwendung, die in drei der beteiligten Städte (Erlangen, Fürth, Nürnberg) zum Einsatz kommt. Wesentlicher Bestandteil ist dabei die elektronische Unterschrift und die Nutzung der elektronischen Geldkarte. Die Anwendung befindet sich im Pilotbetrieb.

Verfahrensbeschreibung

Die Anwendung unterscheidet folgende Fallkonstellationen:

- Neubeantragung eines Anwohnerparkausweises
- Verlängerung eines Anwohnerparkausweises

Teilnehmer des Pilotbetriebs müssen sich zur Beantragung des Anwohnerparkausweises mit Name und Passwort dem System gegenüber mittels qualifizierter elektronischer Unterschrift authentifizieren, da es sich bei der Beantragung eines Anwohnerparkausweises um einen rechtswirksamen Vorgang handelt. Als Bezahlmöglichkeit wird aufgrund der Ähnlichkeit zur Barzahlung die elektronische Geldkarte angeboten. Die Zustellung des Anwohnerparkausweises erfolgt derzeit noch auf postalischem Wege.

Datenverarbeitung

Dienste – wie z.B. Signatur und Bezahlfunktion – werden für alle Städte zentral zur Verfügung gestellt. Die Speicherung und Nutzung der übermittelten Daten erfolgt durch die beteiligten Städte jeweils nur für ihre eigenen Bürger; keine Stadt kann auf die Datenbestände einer anderen beteiligten Kommune zugreifen.
Die übermittelten Daten werden mit den Daten des Einwohnermelderegisters verglichen (spezielle View der Datenbank, nur lesend). Anhand der Rückgabewerte wird automatisch entschieden, ob die Angaben des Antragstellers ausreichend sind oder ob z.B. eine falsche Schreibweise vorliegt. Dem Antragsteller sind keinerlei Einwohnermeldedaten zugänglich.
Die Überprüfung mit den Melderegisterdaten wird erst nach erfolgreicher Signatur des Antrages durchgeführt und wenn zumindest der Name der Signaturkarte mit den eingegebenen Werten übereinstimmt.
Die Vertraulichkeit der Daten wird bei der Übertragung über das Internet durch SSL-Verschlüsselung mit aktuell 128 Bit oder andere Verschlüsselungsverfahren mit der gleichen Verschlüsselungsstärke gewährleistet.
Für die Authentifizierung mit Signaturkarte und für die Bezahlung mit der Geldkarte werden signierte Java-Applets eingesetzt. Cookies werden (nur) temporär zum Sessionmanagement eingesetzt und mit Beendigung der Sitzung aus dem Speicher des Nutzer-PC gelöscht. Die Anwendung funktioniert auch dann, wenn die Annahme von Cookies durch den Nutzer zurückgewiesen wird. Es sind damit lediglich Einbußen im Handhabungskomfort verbunden.

Es werden nur die Daten gespeichert, die benötigt werden, um die Erstellung oder Verlängerung eines Anwohnerparkausweises auszuführen. Zugriffe auf Web-Server werden anonym protokolliert. Die Protokolle (Log-Dateien) werden für die Störungs-

analyse und für anonyme statistische Auswertungen genutzt und nach 30 Tagen gelöscht. Protokolleintragungen, die für den Nachweis und die Durchsetzung von Zahlungsansprüchen benötigt werden, werden spätestens 180 Tage nach vollständiger Zahlung gelöscht.

Datenschutzrechtliche Bewertung:

Das Verfahren nutzt die derzeit verfügbaren technischen Möglichkeiten zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der über Internet übertragenen Daten. Dabei wird auch darauf geachtet, die Datenerhebung und Dauer der Datenspeicherung auf das erforderliche Maß zu begrenzen.

Projektbetreiber:
Curiavant Internet GmbH, Hauptmarkt 17, 90403 Nürnberg
E-Mail: info@curiavant.de

für die Städte Erlangen, Fürth, Nürnberg

7.2.3 Auftrags- und Arbeitsmappe der Stadt Dortmund

Ziel des Projektes Digitale Stadtverwaltung ist es, alle Dienstleistungen und Produkte, die die Stadtverwaltung Dortmund an ihre Bürger und Bürgerinnen erbringt, über das Internet elektronisch verfügbar zu machen. In den Fällen, in denen eine komplette elektronische Abwicklung des Verwaltungsvorgangs derzeit aufgrund rechtlicher Bestimmungen nicht möglich ist, soll zumindest sichergestellt sein, dass die Bürgerinnen und Bürger die erforderlichen Anträge im Rahmen der Internetlösung online erhalten kann, um Wartezeiten und Mehrfachvorsprachen zu verhindern.

Verfahrensbeschreibung:

In die doMap können alle Wünsche, Arbeitsaufträge und Anträge an die Stadtverwaltung eingestellt werden. Um sie benutzen zu können, ist eine einmalige Identifizierung erforderlich. Hier wird geprüft, wer der Besitzer beziehungsweise die Besitzerin ist und die tatsächliche Identität festgestellt. Das erteilte Passwort ermöglicht den Zugang zu doMap und verschlüsselt die Kommunikation mit der Stadtverwaltung. In der Mappe werden die persönlichen Grunddaten (Name, Anschrift, etc.) verwaltet und zur automatischen Übernahme in Formulare bereitgehalten. Auch das Bezahlen (zzt. per Lastschriftauftrag) wird hierüber gesteuert. Weitere Paymentverfahren werden derzeit entwickelt. Sobald ein Auftrag in doMap eingestellt ist, übernimmt ein elektronischer Agent den Arbeitsauftrag und sorgt für seine Erledigung in der Verwaltung. Die Arbeitsergebnisse, egal ob Auskünfte, Stellungnahmen oder Bescheide, werden vom zuständigen Mitarbeiter der Verwaltung wieder in die Mappe eingestellt. Kann der Arbeitsauftrag innerhalb der Verwaltung per EDV elektronisch erledigt werden, stellt die EDV das Arbeitsergebnis automatisch in die Mappe ein.

Datenschutzrechtliche Bewertung:

Die Sicherheit der über das Internet gesendeten Bestands- und Inhaltsdaten wird durch eine 128-Bit-Verschlüsselung gewährleistet. Die Verschlüsselungstiefe von 128-Bit ist der derzeitige Browser-Standard. Sobald eine Verschlüsselungstiefe von 512-Bit oder 1024-Bit möglich ist, wird sie eingesetzt.
Für die Authentifizierung ist ein Login mit Benutzernamen und Pin/Passwort üblich. Die Daten werden verschlüsselt im LDAP-Server abgelegt, wobei die Verschlüsselung nicht umkehrbar ist, sodass niemand in der Lage ist, eine PIN wieder in Klartext zu entschlüsseln. Transaktionen, die eine rechtsgültige Unterschrift verlangen, erfordern eine elektronische Signatur, die jedoch erst für das Jahr 2004 geplant ist. Im Rahmen der Sicherheit der Systeme wird ein zweistufiges Firewall-Konzept verwendet. Die erste Firewall lässt Requests an die Ports 80 und 443 (HTTP und SSL) durch. Diese werden in der Zone zwischen den beiden Firewalls (der so genannten DMZ – Demilitarized Zone) durch den HTTP-Server entgegengenommen und an den Applikationsserver weitergeleitet. Dieser befindet sich hinter einer weiteren Firewall im Intranet. Die Kommunikation zwischen HTTP-Server und Applikationsserver findet dabei in einem anderen Protokoll über einen anderen Port statt. Die DNS-Namen und IP-Adressen der Inhouse-Maschinen sind dabei nach außen hin nicht sichtbar. Die in die doMap vom zuständigen Sachbearbeiter zum Abruf bereitgestellten Arbeitsergebnisse liegen verschlüsselt auf dem Server der Stadt und sind nur von den Nutzerinnen und Nutzern einzusehen. Jedes einzelne Fachverfahren wurde vor Implementie-

rung in die doMap vom Fachamt, dem Personalrat und dem Datenschutzbeauftragten geprüft und gegengezeichnet.

Projektbetreiber:

Stadt Dortmund
Südwall 2-4
44122 Dortmund
www.dortmunder-systemhaus.de und www.dortmund.de

7.2.4 Briefwahlunterlagen über das Internet in Hamburg

Seit der Bürgerschafts- und Bezirksversammlungswahl 2001 haben die Hamburger Bürgerinnen und Bürger die Möglichkeit, neben dem bislang üblichen schriftlichen Antragsverfahren die Briefwahlunterlagen auch elektronisch zu ordern. Das Verfahren wurde auch bei der Vorbereitung der Bundestagswahl 2002 eingesetzt.

Verfahrensbeschreibung

Der Antrag auf Zusendung der Briefwahlunterlagen kann interaktiv über das Internetportal der hamburgischen Verwaltung www.hamburg.de gestellt werden. Für die Authentifizierung der Wahlberechtigten müssen neben Namen und Anschrift auch das Geburtsdatum und die auf der Wahlbenachrichtigungskarte enthaltene Nummer des Wählerverzeichnisses im Bestellformular eingegeben werden.

Datenverarbeitung

Im Wege der Auftragsdatenverarbeitung nimmt die hamburg.de GmbH & Co KG die Daten entgegen und konvertiert sie in verbindlich definierte XML-Datenstrukturen. Diese werden vom Landesamt für Informationstechnik (LIT) in regelmäßigen Abständen in das dortige Rechenzentrum übertragen. Die Antragsdaten werden mit den im Dialogverfahren zur Unterstützung der Wahldienststellen (DIWA) gespeicherten Daten abgeglichen, sodass die bezirklichen Wahldienststellen die beantragten Unterlagen ausstellen und versenden können. Antragstellerinnen und Antragsteller werden elektronisch über die Bearbeitung ihres Antrags informiert. Das der elektronischen Datenverarbeitung zugrundeliegende Serviceflow-Konzept wurde von HiTeC e.V. entwickelt. Zur Schaffung der rechtlichen Voraussetzungen war auch eine Anpassung der Wahlordnung erforderlich, die bis dahin allein die schriftliche Antragstellung vorsah.

Datenschutzrechtliche Bewertung:

In dem Verfahren werden die datenschutzrechtlichen Vorschriften eingehalten. Die von den Antragstellern geforderten Zusatzangaben (Wahlscheinnnummer, Geburtsdatum) werden ausschließlich zur Authentifizierung genutzt. Sie sind im Übrigen der verantwortlichen Stelle ohnehin bekannt. Die Vertraulichkeit der Daten wird bei der Übertragung über das Internet durch SSL-Verschlüsselung gewährleistet. Als kompliziert erwiesen sich die geschachtelten Auftragsverhältnisse zwischen den beteiligten Stellen, wobei als Auftraggeber die Freie und Hansestadt Hamburg, als Auftragnehmer die hamburg.de GmbH&Co KG auftritt, die ihrerseits Unteraufträge an andere Unternehmen vergeben hat. Die Auftrags- und Unterauftragsverhältnisse sind gem. § 3 Hamburgisches Datenschutzgesetz schriftlich geregelt. Alle beteiligten Stellen verpflichteten sich auf ein gemeinsames Datenschutzkonzept.

Projektverantwortung:

Bei der Umsetzung dieses Projekts arbeiteten das Senatsamt für Bezirksangelegenheiten (SfB) –Zentralstelle IuK–, das Landeswahlamt, das Landesamt für Informationstechnik (LIT), der Internet-Provider hamburg.de und das Hamburger Informatik Technologie-Center (HiTeC e.V.) zusammen.

Ansprechpartner:

Freie und Hansestadt Hamburg
Senatsamt für Bezirksangelegenheiten – Zentralstelle IuK
Weidestr. 122c, 22083 Hamburg
Tel. 040-42832.2435 eMail: Juergen.Grandt@sfb.hamburg.de

7.2.5 Fahrscheine in Marburg

In Marburg haben die Stadtwerke auf ihren innerstädtischen Buslinien die herkömmlichen Streifenkarten durch Chipkarten im Scheckkartenformat ersetzt.

Verfahrensbeschreibung:

Die Elektronic-Card Marburg ist eine Chipkarte mit den Funktionen einer elektronischen Fahrkarte und elektronischen Geldbörse. Bei dieser Karte wird die kontaktlose Chipkartentechnologie eingesetzt, d.h. die Karte muss nicht in ein Lesegerät eingesteckt werden, sondern sie kann im Abstand von max. 10 cm am Lesegerät vorbeigeführt werden. Beim Vorbeiführen der Karte am Lesegerät muss gleichzeitig eine Taste bedient werden, damit Doppelbuchungen verhindert werden. Auf der Karte können drei verschiedene Preisstufen gespeichert werden. Setzt der Fahrgast die Karte mit der höchsten Preisstufe auf einer Fahrtstrecke ein, die einer geringeren Preisstufe zugerechnet wird, so muss er die Karte auch beim Aussteigen am Lesegerät vorbeiführen, damit ihm nur der geringere Betrag von der Karte abgebucht wird.
Bei der Karte handelt es sich um eine anonyme Wertkarte, die im voraus aufgeladen werden muss. An den Verkaufsstellen der Stadtwerke kann sie bis maximal 200 Euro geladen werden, in allen Bussen bis 25,00 Euro. Gespeichert sind auf der Karte die Kartennummer und Informationen zur letzten durchgeführten Fahrt wie Datum, Uhrzeit, Fahrpreis, Starttarifgebiet, Starthaltestelle, Gerätenummer, Guthaben, Benutzbarkeit (zwei Jahre seit dem letzten Aufladen) und Zielhaltestelle, soweit das Gerät erneut betätigt wird. Für den Kunden ablesbar sind davon an den Lesegeräten im Bus allerdings lediglich Datum, Uhrzeit und Fahrpreis der letzten Fahrt, Tarifgebiet der letzten Fahrt, Guthaben und Benutzbarkeit.
Die Kunden können die Karten bei allen Verkaufsstellen der Stadtwerke gegen Hinterlegung eines Pfands erhalten. Bei Kartenverlust bieten die Stadtwerke zwei verschiedene Zahlungswege an, die dem Kunden ein Wahlrecht zwischen Deanonymisierung und Anonymität lassen. Zunächst ist es unerlässlich, die Pfandquittung vorzulegen, auf der die Kartennummer notiert ist. Ohne Pfandquittung gibt es keine Erstattung von Pfand oder noch auf der Karte gebuchten, bereits bezahlten Geldbeträgen. Dann hat der Kunde die Möglichkeit, sich nach ca.14 Tagen einen Verrechnungsscheck schicken zu lassen mit der Folge der Deanonymisierung. Alternativ kann er die noch verbuchten Beträge und Pfand nach 14 Tagen bei einer Verkaufsstelle persönlich ohne Namensnennung abholen. Die 14-Tages-Frist wird benötigt, um die Karte auf mögliche Manipulationen zu überprüfen.

Datenschutzrechtliche Bewertung:

Die Ausgestaltung dieser Karte, die anonym erworben und genutzt werden kann, ist datenschutzrechtlich nicht zu beanstanden. Die Kunden können sämtliche Fahrten anonym zurücklegen. Selbst bei Verlust der Karte ist eine Erstattung der Restbeträge möglich, ohne dass der Inhaber der Karte seine Identität preisgeben müsste. Bewegungsprofile sind bei diesem System ausgeschlossen.

Projektbetreiber:
Stadtwerke Marburg – Hauptverwaltung, Am Krekel 55, 35039 Marburg
eMail: info@swmr.de

7.2.6 Fundsachen (Verlust-/Fundanzeige) in Schwabach

Die Online-Anwendung Fundsachen (Verlust-/Fundanzeige) der Stadt Schwabach ist im Produktiveinsatz. Bisher wurde dies über ein weitgehend formloses schriftliches oder telefonisches Verfahren abgewickelt.

Verfahrensbeschreibung

Über Online-Formulare werden personen- und fachspezifische Daten (Pflichtangaben und freiwillige Angaben) erhoben. Erklärungen und Hinweise werden ebenfalls im Rahmen der Online-Formulare gegeben. Eine besondere Authentifizierung oder eine elektronische Unterschrift sind nicht erforderlich, da diese Anträge bzw. Anzeigen bereits heute telefonisch möglich sind. In beiden Verfahren werden mit Antrag/Anzeige auch keine unmittelbaren Gebühren wirksam. Der Einstieg erfolgt über eine Seite mit Informationen zum Thema Fund- und Verlustanzeige. Aus dieser Einstiegsseite wird verlinkt auf:

- Erläuterungen des Fundamtes,
- Datenschutzhinweise.

Datenverarbeitung

Die Daten werden in der Online-Anwendung auf Vollständigkeit geprüft und strukturiert zusammengestellt. Die Verbindung zum Webserver wird grundsätzlich SSL-verschlüsselt (128 Bit, SSL-Zertifikat). Es werden nur die für die Sachbearbeitung erforderlichen Daten erhoben. Die Abgabe von Erklärungen bzw. die Bestätigung einer Kenntnisnahme von Hinweisen wird durch aktives Anklicken von Checkboxen realisiert. Werden diese Bestätigungen nicht abgegeben, werden entsprechende Fehler- bzw. Hinweismeldungen von der Anwendung ausgegeben und der Online-Vorgang kann nicht abgeschlossen werden. Sind alle Daten vollständig, werden diese in einer Übersicht, die zusätzlich auch in druckfreundlichem Format angeboten wird, zusammengestellt und können vom Nutzer nochmals überprüft und ggf. korrigiert werden. Die Daten werden per eMail an eine definierte Adresse der Dienststelle verschickt. Die Verbindung zum Mailserver der Kommune erfolgt über VPN. Die Datenspeicherungen sind auf ein Jahr begrenzt.

Datenschutzrechtliche Bewertung:

Das Verfahren nutzt die derzeit verfügbaren technischen Möglichkeiten zur Sicherstellung von Vertraulichkeit und Integrität der über Internet übertragenen Daten. Maßnahmen zur Sicherstellung der Authentizität sind nicht erforderlich. Das Verfahren zeigt überdies Möglichkeiten zur Umsetzung der Forderungen des Teledienstedatenschutzgesetzes (TDDSG) auf.

Projektbetreiber:
Curiavant Internet GmbH, Hauptmarkt 17, 90403 Nürnberg
eMail: info@curiavant.de

7.2.7 Fundsachenverwaltung in Hamburg

Mit der Anwendung FundInfo steht in der Freien und Hansestadt Hamburg ein Verfahren zur Verwaltung von Fundsachen zur Verfügung, das über eine Internetanwendung auch die Suche nach verloren gegangenen Gegenständen durch den Bürger ermöglicht.

Verfahrensbeschreibung

Personenbezogene Angaben werden vom Fundbüro erhoben und in einer zentralen Datenbank gespeichert, wenn ein Finder einen Fund anzeigt bzw. ein Eigentümer einen Verlust meldet. Bei dieser mandantenfähigen ASP-Anwendung greift das Fundbüro über das Internet auf die Daten zu, die in einem kommunalen Rechenzentrum gespeichert werden. Im Rahmen der Bürgersuche kann der Suchende über das Internet ausschließlich den öffentlichen Teil der beim Rechenzentrum gepflegten Daten abrufen. Auf diesem Weg besteht nur ein lesender Zugriff auf diese Daten. Zur weitergehenden Klärung, ob es sich bei einem der angezeigten Funde tatsächlich um den verlorenen Gegenstand handelt, muss der Bürger direkt mit dem Fundbüro persönlich, telefonisch, schriftlich oder per Mail Kontakt aufnehmen.

Datenschutzrechtliche Bewertung:

Die demilitarisierten Zonen des kommunalen Rechenzentrums bilden die Basis für die Datensicherheit bei der Anwendung FundInfo.
Im Rahmen der Fundsachenverwaltung durch das Fundbüro können auch sensible Daten wie z.B. besondere Fundorte oder Fundbeschreibungen durch das Fundbüro erfasst und über eine Internetverbindung zum kommunalen Rechenzentrum übertragen werden. Die Vertraulichkeit der Daten wird über eine SSL-Verschlüsselung gewährleistet. Der Zugriff auf die Daten wird durch individuellen Kennungen und Passworte geschützt. Durch die Kontrolle der IP-Adresse wird sichergestellt, dass der Zugriff auf alle Daten, die zu einer Fundssache gehören, nur aus dem verwaltungsinternen Netz heraus erfolgen kann.
Durch die Festlegung, welche Datenfelder bei der öffentlichen Bürgersuche angezeigt werden und durch die getroffenen organisatorischen Regelungen, in welcher Art und Weise, Fundsachen beschrieben werden, wird sichergestellt, dass keine sensiblen Daten öffentlich angezeigt werden.
Die Bürgersuche kann anonym genutzt werden; es ist kein spezieller Account erforderlich. Die Suchanfragen erfolgen über Auswahlfelder und zum Teil über freie Eingabefelder. Da bei der Suchanfrage zum Teil auch sensible Daten eingegeben werden können, werden die Daten bei der Übertragung mit SSL verschlüsselt.

Projektverantwortung:

Freie und Hansestadt Hamburg
Bezirksamt Hamburg - Mitte
Klosterwall 8
20095 Hamburg
Telefon: 040/428 54 - 0
Fax: 040/428 54 – 45 40

7.2.8 Grundbuch in Mecklenburg-Vorpommern

Mit der Verabschiedung des Registerverfahrensbeschleunigungsgesetzes im Jahr 1993 hat der Gesetzgeber die Grundlagen dafür geschaffen, das Grundbuch nicht mehr nur ausschließlich in Papierform führen zu können. Seitdem ist es zulässig, den Rechtsbestand des Grundbuchs elektronisch abzubilden. Im Auftrag des Justizministeriums Mecklenburg-Vorpommern wurde ein Verfahren entwickelt, mit dem das Grundbuch künftig elektronisch geführt werden soll. Weil damit unter anderem erreicht wird, dass der Datenbestand gleichzeitig an verschiedenen Stellen beliebig oft zur Verfügung steht, erhofft sich das Ministerium insbesondere bei der Grundbuchauskunft einen erheblichen Rationalisierungseffekt.

Rechtliche Grundlagen

Neben einer Reihe von Verfahrensvorschriften sind die §§ 75 Grundbuchverfügung (GBV) und 126 Grundbuchordnung (GBO) aus datenschutzrechtlicher Sicht von besonderer Bedeutung. § 75 GBV fordert unter anderem, dass eine Eintragung nur möglich sein soll, wenn die zur Führung des Grundbuches zuständige Person der Eintragung ihren Namen hinzusetzt und beides elektronisch unterschreibt. Dabei soll die elektronische Unterschrift in einem allgemein als sicher anerkannten automatisierten kryptographischen Verfahren hergestellt werden und von der zuständige Stelle überprüft werden können. Nach § 126 GBO muss darüber hinaus gewährleistet sein, dass die Eintragungen auf Dauer inhaltlich unverändert in lesbarer Form wiedergegeben werden können. An die Integrität und die Verfügbarkeit der elektronisch gespeicherten Grundbuchdaten werden also höchste Ansprüche gestellt.

Verfahrensbeschreibung

Das Elektronische Grundbuch (EGB) wird auf einem zentralen Serversystem im Hochsicherheitsbereich des Landesrechenzentrums geführt. Der Rechtspfleger im Grundbuchamt (GBA) kommuniziert mit Hilfe seines Client-PC über das GBA-LAN mit dem GBA-Server sowie über das LAN, einen speziell eingerichteten Knotenrechner (Router) und das Landesdatennetz mit dem zentralen Server. Die Router sorgen für eine verschlüsselte Kommunikation über das WAN. Zur Realisierung der elektronischen Unterschrift erhält jeder Rechtspfleger eine personenbezogene SmartCard, auf der sein privater Signaturschlüssel abgelegt ist. Der Client-PC im GBA verfügt über ein entsprechendes SmartCard-Lesegerät. Die Eintragung in das EGB erfolgt erst, nachdem der Rechtspfleger den Eintragungstext mit seinem privaten Schlüssel digital signiert hat und die Gültigkeit des Schlüssels anhand der Einträge in die Datenbank der Zertifizierungsstelle geprüft wurde. Die Signatur stellt die von § 75 GBV geforderte Elektronische Unterschrift dar. Text und Signatur gemeinsam bilden den Eintrag in das EGB im Sinne von § 75 GBV. Die elektronisch unterschriebenen Einträge in der EGB-Datenbank werden zusätzlich durch einen Security-Server abgesichert, der eine eigene elektronische Unterschrift je Eintrag erzeugt und verwaltet. Eine Nachsignierung der EGB-Einträge – etwa wegen nicht mehr als sicher bewerteter Signaturalgorithmen – erfolgt durch Ersetzen der entsprechenden Einträge im Security-Server.

Datenschutzrechtliche Bewertung:

Aus datenschutzrechtlicher Sicht ist von besonderer Bedeutung, dass nur berechtigte Personen Einträge in des EGB realisieren können. Dies wird dadurch gewährleistet, dass sich jeder Rechtspfleger mit seiner personenbezogenen SmartCard zweifelsfrei gegenüber dem EGB authentisiert. Die Eingabe der PIN vor jedem Eintragungsvorgang stellt sicher, dass tatsächlich ein berechtigter Nutzer den jeweiligen Eintrag vornimmt.
Die Forderungen des § 75 GBV nach einer elektronische Unterschrift in einem allgemein als sicher anerkannten automatisierten kryptographischen Verfahren werden erfüllt. Die Integrität der Einträge wird einerseits durch die elektronische Unterschrift des Rechtspflegers und andererseits durch die zusätzliche Signatur auf dem Security-Server sichergestellt. Das geplante Verfahren zur Nachsignierung soll dafür sorgen, dass die Integrität der Einträge auch dann gewährleistet bleibt, wenn ein Signaturalgorithmus wegen der technischen Entwicklung nicht mehr als sicher bewertet werden kann. Die Vertraulichkeit bei der Übertragung über das WAN wird durch die Verschlüsselung der Daten gewährleistet. Die sensiblen Grundbuchdaten werden auf dem zentralen Server im Hochsicherheitsbereich des Landesrechenzentrums gespeichert und sind somit einerseits vor unberechtigten Zugriffen geschützt. Andererseits werden damit die hohen Anforderungen an die Verfügbarkeit der Grundbuchdaten erfüllt. Die Verfügbarkeit über den geforderten sehr langen Zeitraum soll durch ein Datenbankmanagementsystem mit aufwändigen Archivierungs-, Backup- und Recoverykonzepten und durch die Verwendung von Textformaten, die unabhängig von gängiger Standardsoftware gelesen werden können, sichergestellt werden.

Projektbetreiber

Justizministerium Mecklenburg-Vorpommern
19048 Schwerin
Ansprechpartner:
Dr. Kai Jaspersen
Tel: 0385/588-3152
eMail: dr.kai.jaspersen@jm.mv-regierung.de

7.2.9 Hundesteuer in Krefeld

Die Stadt Krefeld bietet neben diversen anderen Online-Anträgen auch die Möglichkeit, eine Anmeldung zur Hundesteuer abschließend über das Internet vorzunehmen. Das Verfahren umfasst die Anmeldung von bis zu zwei Hunden im Rahmen der Hundesteuerpflicht (ohne rechtsverbindliche Steuerbefreiung/-ermäßigung). Nach der Hundesteuersatzung der Stadt bedarf die Anmeldung keiner besonderen Form. Die Online-Anmeldung ist daher auch ohne elektronische Signatur rechtmäßig möglich.

Datenverarbeitung:

Informationen und die dem Antrag zugrunde liegenden Rechtsgrundlagen sind ohne Angabe von persönlichen Daten für jede/n Interessierte/n erreichbar. Im Antrag werden nur solche Daten erhoben und gespeichert, die für den Einzelfall zutreffend und für das weitere Verfahren notwendig sind. Hierüber wird der Nutzer und die Nutzerin im Impressum und mit Aufruf des Formulars informiert. Die Eingabe aller Daten ist freiwillig. Unmittelbar nach der Speicherung wird das Antragsdokument automatisiert in eine andere Datenbank kopiert und in der Ursprungsdatenbank gelöscht. Der Weg des Dokumentes kann vom Internet aus nicht nachvollzogen werden. Die Antragsdatenbank ist darüber hinaus nicht über Hyperlinks zu erreichen. Ein Ausspionieren der eingegangenen Daten über das Internet ist damit faktisch ausgeschlossen. Eine Weitergabe von Daten an Dritte findet nicht statt. Die Speicherung richtet sich nach den bestehenden gesetzlichen Vorschriften. Anonymisierte Daten über die Nutzerinnen und Nutzer der Krefelder Internetpräsentation werden in Log-Dateien gespeichert. Durch die Verkürzung der IP-Adressen um die letzten drei Ziffern ist ein Rückschluss auf den einzelnen Nutzer und die Nutzerin ausgeschlossen. Die Log-Dateien werden ausschließlich für Zwecke der Datensicherheit und für statistische Zwecke erhoben und nach zwei Monaten gelöscht.

Datenschutzrechtliche Bewertung:

Das Verfahren entspricht den datenschutzrechtlichen Vorgaben. Die Eingaben werden verschlüsselt übermittelt. Dadurch sind sie vor der Kenntnisnahme Dritter und Verfälschung geschützt. Eingesetzt wird eine SSL-Verschlüsselung mit 128 Bit Verschlüsselungsstärke, die auch zukünftig weiter der fortschreitenden technischen Entwicklung angepasst werden wird. Der Zugriff auf den eingegangenen Online-Antrag und die darin enthaltenen Personenbezogenen Daten ist ausschließlich dem/der zuständigen Bearbeiter/in des Fachbereichs/Fachamtes eingeräumt. Der Personenkreis, dem der Inhalt eines eingegangenen Onlineantrags bekannt wird, ist damit kleiner als der, der Kenntnis vom schriftlichen Posteingang erhält.

Projektbetreiber:

Oberbürgermeister der Stadt Krefeld
Konrad-Adenauer-Platz 17
47792 Krefeld
www.krefeld.de; stadtservice@krefeld.de

7.2.10 Internetportal niedersachsen.de

Für eine Reihe von Diensten und Objekten (Mailserver, Backupmanagement, Systemmanagement, Name Services und Firewall) konnte auf der vorhandenen Infrastruktur aufgesetzt werden. Da der Aufbau und die Absicherung dieser Dienste nicht Gegenstand der Untersuchung niedersachsen.de war, erfolgt keine weitere Betrachtung. Sollten entsprechende Konzepte noch nicht vorliegen, wird empfohlen diese zu erstellen, da diese Dienste umfangreiche Auswirkungen haben könnten.

Technische Rahmenbedingungen:

- Zentrales Content Management System im Informatikzentrum Niedersachsen (izn),
- Dezentrale Eingabe durch Redakteure der Dienststellen (über iznNet) über browserbasierte Applikation,
- Workflow basiert auf Vier-Augen-Prinzip: Eingabe durch Redakteure, Freigabe durch Chefredakteure,
- Verschlüsselung der Kommunikation zwischen Client und CMS über https.

Inhaltsdaten:

- Bedienstetendaten: Veröffentlichung nur, wenn der Dienstverkehr es erfordert oder mit Einwilligung des Bediensteten (Rechtsgrundlage in Nds. § 101 NBG),
- Bürgerdaten: Veröffentlichung nur mit Einwilligung der Bürger.

Nutzungsdaten:

- Formulardaten: Beschränkung auf das notwendige Maß,
- IP-Adressen: Beschränkung auf die ersten drei Ziffern,
- Verzicht auf Cookies.

Datenschutzrechtliche Bewertung:

Das Informationsangebot niedersachsen.de zeichnet sich durch ein überzeugendes datenschutzfreundliches Konzept aus. Interessierte aus Verwaltung und Wirtschaft sowie Bürgerinnen und Bürger, die mit dem Informationsanbieter niedersachsen.de über das Internet kommunizieren wollen, können sicher sein, dass das für die Sicherheit Notwendige getan worden ist.

Projektbetreiber:

Nds. Staatskanzlei - Presse- und Informationsstelle der Landesregierung –, Planckstraße 2, 30169 Hannover – Telefon: 0511-120-0
Ansprechpartner:
Dr. Walter Swoboda
Tel.: (0511) 120-6950
Email: walter.swoboda@stk.niedersachsen

7.2.11 Jobbörse Niedersachsen online

Die 1996 auf der Grundlage der mit den Gewerkschaften und Berufsverbänden zur sozialverträglichen Umsetzung der Verwaltungsreform getroffenen Vereinbarungen eingerichtete „Jobbörse Niedersachsen“ hat die Aufgabe, die Landesbediensteten, die von Maßnahmen der Staatsmodernisierung betroffen sind und deshalb ihre bisherigen Arbeitsplätze nicht mehr wahrnehmen können (z.B. durch Auflösung von Landesbehörden oder Umstrukturierungsmaßnahmen), und Mitarbeiterinnen und Mitarbeiter, die an einer anderen Verwendung interessiert sind, bei der Suche nach einem neuen Arbeitsplatz zu unterstützen. Mit der Einführung des automatisierten Verfahrens „Job-Börse online“ können Dienststellen die freien und besetzbaren Dienst- und Arbeitsplätze über das Landesintranet in den Stellenpool einstellen und die Bewerberinnen und Bewerber ihr individuelles Bewerbungsprofil hinterlegen. Die Daten des Stellenpools und die individuellen Bewerberprofile werden in einer zentralen Datenbank gespeichert, um zum Zwecke eines Abgleichs der Stellen- und Bewerbungsprofile individuell und zielgerichtet ausgewertet werden zu können.

Verfahrensbeschreibung

Die MS-Access-Datenbank „Job-Börse Niedersachsen“ wird bei den Bezirksregierungen Braunschweig, Hannover, Lüneburg und Weser-Ems unter dem Betriebssystem Windows NT eingesetzt. Die System- und Programmsystemadministration erfolgt zentral. Die Anwendung steht allen zur Verfügung, die Zugang zum Intranet des Landes Niedersachsen haben. Das tagesaktuelle Stellenangebot ist für jeden Bediensteten des Landes über das Landesintranet ohne Passwort-Abfrage mit einem reinen Lesezugriff möglich. Darüber hinaus ist ein passwort-geschützter Zugang für die Eingabe und Pflege der Datenbestände für die meldenden Dienststellen, für Reformbetroffene und Job-Suchende vorgesehen. Ein Matching zwischen zwischen Stellen- und Bewerberprofil ist möglich; individuelle Stellenangebote werden den Bewerberinnen und Bewerber per eMail zugesandt.

Datenschutzrechtliche Bewertung:

Die Vertraulichkeit der über das Intranet übermittelten Daten wird durch die Verschlüsselung der Daten gewährleistet (SSL-128-Bit-Verschlüsselung). Die Eingabe von Benutzerkennung und Passwort stellt sicher, dass tatsächlich ein berechtigter Nutzer den Eintrag und die Pflege vornimmt.
Die Bewerberdaten werden auf Servern der Bezirksregierungen vorrätig gehalten. Die Datensicherheit und die Verfügbarkeit sind gewährleistet.
Ein detailliertes Berechtigungskonzept für die zentrale und dezentrale Administration sowie für die Einsicht in das eigene Bewerberprofil liegt vor.
Die im Bewerberprofil erhobenen Pflichtdaten sind auf den für den Vermittlungszweck und den Abgleich mit dem Stellenangebot erforderlichen Umfang begrenzt. Zusätzliche freiwillige Angaben der Bewerber sind in der dafür erforderlichen Eingabemaske eindeutig gekennzeichnet. Freiwillige Angaben werden durch die Job-Börse erst dann zur weiteren Verarbeitung freigegeben, wenn die Bewerberinnen und Bewerber der Job-Börse innerhalb von vier Wochen schriftlich ihr Einverständnis zur Verarbeitung dieser Daten erklärt haben. Die Einwilligung in die Verarbeitung der freiwilligen Angaben kann von den Bewerberinnen und Bewerbern jederzeit mit Wirkung für die Zu-

kunft widerrufen werden. Nicht Reformbetroffene, die das Angebot der Job-Börse nutzen wollen, um sich über Stellenangebote zu informieren, wird alternativ die Möglichkeit eröffnet, sich unter Pseudonym bei der Job-Börse zu bewerben.
Eine frühestmögliche Löschung der Berwerberdaten ist sichergestellt.
Die Datenfelder, die darüber hinaus in anonymisierter Form für Statistikzwecke zur Verfügung stehen sollen, werden eindeutig definiert.

Weitergehende konkretisierende datenschutzrelevante Regelungen werden in Kürze in einer Vereinbarung nach § 81 NPersVG mit den Gewerkschaften festgelegt. Bestandteile sind der Datenkatalog, die Bewerberprofile, die Verarbeitungs- und Auswertungsmöglichkeiten der Software, Protokollierungsmöglichkeiten und die Betroffenenrechte.

Projektverantwortung

Niedersächsisches Innenministerium
Personalreferat
Frau Angela Schilling
Telefon: 0511-120-6451
EMail: angela.schilling@mi.niedersachsen.de

7.2.12 Liegenschaftsbuch in Brandenburg

Wie in anderen Bundesländern wird auch in Brandenburg seit einigen Jahren das Liegenschaftskataster weitgehend in elektronischer Form geführt. In dieser Form stehen einerseits das automatisierte Liegenschaftsbuch (ALB) sowie andererseits die automatisierte Liegenschaftskarte (ALK) zur Verfügung. Im Rahmen einer eGovernment-Lösung kann nunmehr auf das ALB online zugegriffen werden. Der Landesbetrieb „Landesvermessung und Geobasisinformation Brandenburg“ (LGB) sowie das Ministerium des Innern Brandenburg haben zu diesem Zweck das Verfahren ALBonline entwickelt, mit dem bestimmte institutionelle Nutzer des Liegenschaftskatasters die Möglichkeit erhalten sollen, auf die im ALB gespeicherten Daten über das Internet zugreifen zu können. Dabei ist nicht vorgesehen, das ALB für die Allgemeinheit zu öffnen und in das Internet einzustellen. Dies wäre nach Brandenburgischem Vermessungs- und Liegenschaftsrecht auch nicht zulässig, da die im ALB gespeicherten personenbezogenen Eigentümerdaten nur bei einem berechtigten Interesse herausgegeben werden dürfen. Der Landesbetrieb beabsichtigt daher, nur denjenigen Nutzern einen Zugriff auf das ALB zu eröffnen, die gesetzlich befugt sind, das ALB automatisiert abzurufen. Dazu gehören beispielsweise die öffentlich bestellten Vermessungsingenieure, Notare, aber auch die Ämter und Gemeinden des Landes. Nach § 2 der Brandenburgischen Liegenschaftskataster-Datenübermittlungsverordnung (LiKaDÜV) i. V. m. § 10 des Brandenburgischen Datenschutzgesetzes (BbgDSG) sind eine Reihe von technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen. Der Landesbetrieb hat zu diesem Zweck eine Rechnerarchitektur entwickelt, die die angemessenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik im Wesentlichen berücksichtigt. Die bei den Kataster- und Vermessungsämtern gespeicherten ALB-Daten werden täglich über das Landesverwaltungsnetz und eine Firewall auf einen Datenbankserver im Landesbetrieb überspielt, wodurch die Aktualität des Liegenschaftsbuches gewährleistet wird. Der Nutzer von ALBonline muss zunächst schriftlich die Zulassung zum Online-Verfahren beantragen. Mit Bewilligung des Antrages wird ihm eine Nutzerkennung sowie ein Passwort zugeteilt. Der Zugang zum Webserver des Landesbetriebes ist nur über eine Firewall möglich. Die Daten einschließlich Nutzerkennung und Passwort werden mit dem Verfahren SSL und einer Schlüssellänge von 128 Bit verschlüsselt. Webserver und Datenbankserver sind gegen unbefugte Zugriffe noch einmal besonders gesichert. Die Kommunikation erfolgt ausschließlich in HTML über das Protokoll http. Aktive Inhalte (Java-Applets, ActiveX) werden nicht verwendet. Die Nutzerführung erfolgt über temporäre Cookies, die nach Ende der Sitzung gelöscht werden. Es erfolgt ein lesender Zugriff auf die Datenbank des ALB, deren Veränderung ist nicht möglich.

Datenschutzrechtliche Bewertung:

Das in Brandenburg eingeführte Verfahren ALBonline, mit dem autorisierte Nutzer auf Liegenschaftsdaten über das Internet zugreifen können, genügt den Datenschutzanforderungen sowohl aus rechtlicher als auch aus technischer und organisatorischer Sicht.

Ansprechpartner

Landesvermessung und Geobasisinformation
Brandenburg
Technische Stellen ALB/ALK
Heinrich-Mann-Allee 103
14473 Potsdam
Tel.: (0331) 8844-0
Fax: (0331) 8844-126
eMail: lvermabb@brandenburg.de

7.2.13 Liegenschaftskataster in Niedersachsen

Informationssysteme: Auskunftssystem – InterASL

Mit dem **Inter**netbasierten **A**uskunft**S**ystem des **L**iegenschaftskatasters (**InterASL)** werden die Angaben des amtlichen Vermessungswesens durch die Niedersächsische Vermessungs- und Katasterverwaltung bereitgestellt. Für eine Reihe von Diensten und Objekten (Mailserver, Backupmanagement, Systemmanagement, Name Services und Firewall) konnte auf der vorhandenen Infrastruktur aufgesetzt werden. Da der Aufbau und die Absicherung dieser Dienste Gegenstand der niedersächsischen IuK – Infrastruktur sind, erfolgt keine weitere Betrachtung.

Technische Rahmenbedingungen:

- Zugriff vom Client erfolgt über Java-Applets, die mit dem Geodatenserver über fest definierte Ports und SSL (secure socket layer) kommunizieren.
- Internetserver im Grenznetz des izn-net2000 (demilitarisierte Zone).
- Zurzeit keine Verbindung zwischen Internet und Intranet; ggf. Verbindung zum Intranet über http-Protokoll und fest definierte Ports sowie SSL (secure socket layer) entsprechend Landessystemkonzept angestrebt.

Inhaltsdaten:

- Angaben des amtlichen Vermessungswesens: Abruf möglich mit Ausnahme datenschutzrechtlich sensibler Eigentumsangaben.
- Eigentumsangaben: Abruf nur bei berechtigtem Interesse; wird über hinterlegte Nutzerprofile gesteuert.

Nutzungsdaten:

- Formulardaten: Beschränkung auf das notwendige Maß.
- Benutzerkennung, Passwort, ggf. IP-Adresse.
- Verzicht auf Cookies durch Benutzer möglich.

Datenschutzrechtliche Bewertung:

Mit der Neufassung des Niedersächsischen Vermessungs- und Katastergesetzes erfolgt in Übereinstimmung mit dem Datenschutzrecht eine Liberalisierung des Abrufs der Daten. Der spezialgesetzliche Verwendungsschutz wird über im System hinterlegte Nutzerprofile gewährleistet. Die Protokollierung der Zugriffe stellt eine umfassende datenschutzrechtliche Kontrolle über den Datenabruf sicher und liefert die Parameter für die Abrechnung. Berechtigte Nutzer aus Verwaltung und Wirtschaft sowie künftig auch Bürgerinnen und Bürger, die das Auskunftssystem im Internet nutzen wollen, können sicher sein, dass das für die Sicherheit Notwendige getan worden ist.

Projektbetreiber:

Nds. Innenministerium - Referat 16, Lavesallee 6, 30169 Hannover
Ansprechpartner: Rolf Ueberholz – Telefon: 0511-120-6515
rolf.ueberholz@mi.niedersachsen.de

7.2.14 Melderegisterauskunft der Landeshauptstadt Hannover

Die Anwendung „Einfache Melderegisterauskunft“ unterscheidet drei Fallkonstellationen:

1. Auskünfte an jedermann auf anonyme Anfrage mit Bezahlung der Gebühren per Geldkarte,
2. Auskünfte auf Anfragen von Mitarbeitern registrierter privater Stellen (Firmen, Freiberufler usw.) mit Sammelabrechnung der Gebühren,
3. Gebührenfreie Auskünfte auf Anfragen von Mitarbeitern von Behörden oder sonstigen öffentlichen Stellen.

Personen der Fallgruppen 2 und 3 müssen sich bei der Anfrage durch die elektronische Signatur identifizieren (qualifiziertes Zertifikat eines angezeigten oder akkreditierten Zertifizierungsdiensteanbieters, starke Authentifizierung), wobei dies auch pseudonym erfolgen kann. Die Authentifizierung ist zum Nachweis der Kostenübernahmepflicht der registrierten privaten Stelle bzw. der Eigenschaft als Behördenmitarbeiter erforderlich. Die folgenden datenschutzrechtlichen Belange sind bei der Umsetzung der im Kapitel 5 beschriebenen Handlungsempfehlungen in besonderer Weise berücksichtigt worden:

Nur erforderliche Daten werden gespeichert

Es werden nur die Daten gespeichert, die benötigt werden, um die jeweilige Dienstleistung auszuführen und abzurechnen. Der Abruf von allgemeinen Informationen, etwa zu Angeboten und zu den Anspruchvoraussetzungen, ist ohne Registrierung und Anmeldung möglich. Zugriffe auf Web-Server werden anonym protokolliert. Die Protokolle (Log-Dateien) werden für die Störungsanalyse und für anonyme statistische Auswertungen genutzt. Zu Abrechnungszwecken werden nur Daten verarbeitet und gespeichert, die für den Nachweis und die Durchsetzung des Zahlungsanspruchs benötigt werden. Wenn der Nutzer selbst zahlungspflichtig ist und nicht mit einer Geldkarte zahlt, wird der Name, die Anschrift und der Zahlungsgrund, z.B. „Einfache Melderegisterauskunft am 01.01.2002 12:00 Uhr“ gespeichert. Eine Kontoverbindung wird nur gespeichert, wenn eine Bankeinzugsermächtigung erteilt werden soll. Wenn der Nutzer im Auftrag eines Dritten, z.B. des Arbeitgebers, kostenpflichtige Leistungen in Anspruch nimmt, werden Merkmale gespeichert, die die Berechtigung belegen. Das muss nicht unbedingt der Name sein, das kann auch eine Personalnummer oder ein Pseudonym sein, wenn das so mit dem Zahlungspflichtigen vereinbart worden ist.

Speicherung nicht länger als nötig

Log-Dateien werden nach 30 Tagen gelöscht. Protokolleintragungen, die für den Nachweis und die Durchsetzung von Zahlungsansprüchen benötigt werden, werden spätestens 180 Tage nach vollständiger Zahlung gelöscht; diese Frist ist durch das Haushalts- und Kassenwesen vorgegeben Die Speicherung anderer Daten richtet sich nach den bestehenden gesetzlichen Vorschriften.

Keine Verwendung für andere Zwecke

Die Daten werden nur für den Zweck verarbeitet, für den sie erhoben werden. Eine Verwendung erfolgt nicht für andere dienstliche Zwecke und eine Weitergabe an an-

dere Behörden oder Firmen und Personen erfolgt nur dann, wenn dafür eine gesetzliche Grundlage besteht.

Sichere Verbindung

Bei der Anwendung werden persönliche Daten verschlüsselt übermittelt und somit gegen die Kenntnisnahme durch Dritte geschützt. Eingesetzt werden eine SSL (Secure Socket Layer)-Verschlüsselung mit 128 Bit oder andere Verschlüsselungsverfahren mit der gleichen Verschlüsselungsstärke. Dazu ist es jedoch erforderlich, dass der Browser auf dem Anwender-PC diese Verschlüsslungsstärke unterstützt.

Besonderheit

Das Niedersächsische Meldegesetz (NMG) (Nds. GVBl. 1998 S. 57) bietet noch keine Rechtsgrundlage, Melderegisterauskünfte online über das Internet zu erteilen. Eine entsprechende Anpassung des Niedersächsischen Meldegesetzes an § 21 des Melderechtsrahmengesetzes ist in Kürze zu erwarten. Andererseits ist die Online-Auskunft durch das geltende Recht nicht ausdrücklich untersagt; unter bestimmten Einschränkungen, die unter dem Begriff „Adressbuchlösung“ zusammengefasst werden, wird sie auch jetzt für zulässig gehalten. Zwar macht § 12 Abs. 1 des Niedersächsischen Datenschutzgesetzes (NDSG) in der Fassung vom 29.01.2002 (Nds. GVBl. S. 22) die Zulässigkeit des automatisierten Datenabrufs von einer (ausdrücklichen) gesetzlichen Zulassung abhängig und § 12 Abs. 4 NDSG untersagt sogar, personenbezogene Daten für Personen und Stellen außerhalb des öffentlichen Bereichs zum Abruf bereitzuhalten. Allerdings gelten die Einschränkungen der Absätze 1 bis 4 nicht für den Abruf aus solchen Datenbeständen, deren Inhalt veröffentlicht werden darf. Für Daten aus dem Melderegister kommt die Veröffentlichung in Adressbüchern in Frage; im Umfang der Datenweitergabe an Adressbuchverlage ist somit auch die Online-Melderegisterauskunft zulässig. Gegenüber der Einfachen Melderegisterauskunft in anderer Form sind deshalb bei der Online-Auskunft zurzeit die Einschränkungen von § 34 Abs. 4 und 5 NMG zu beachten: Es dürfen lediglich Auskünfte über Einwohnerinnen und Einwohner erteilt werden, die das 18. Lebensjahr vollendet haben und der Weitergabe an Adressbuchverlage nicht widersprochen haben. Die Ankopplung an die Adressbuchregelung schließt auch Auskünfte über ehemalige Einwohnerinnen und Einwohner (Wegzugadressen) und Verstorbene aus.

Datenschutzrechtliche Bewertung:

Die LHH hat für die häufig nachgefragte Dienstleistung der einfachen Melderegisterauskunft ein automatisiertes Abrufverfahren über das Internet entwickelt, das im Einklang mit den bereichsspezifischen und allgemeinen Datenschutzregelungen steht. In dem Verfahren wird mit den persönlichen Daten des Nutzers vorbildlich umgegangen. Wesentlicher Bestandteil ist dabei die elektronische Signatur und die Möglichkeit der anonymen Zahlung.

Projektbetreiber:

Landeshauptstadt Hannover - Amt für Zentrale Dienste, Abteilung für Informations- und Kommunikationstechnik, Leinstraße 14, 30159 Hannover
eMail: 10.5@Hannover-Stadt.de
(siehe auch Roßnagel/Yildirim, Online-Melderegisterauskunft, DuD 10/2002, 611-614)

7.2.15 Melderegisterauskunft der Region Nürnberg

Im Rahmen des MEDIA@Komm-Projektes der Region Nürnberg wurde für die häufig nachgefragte Dienstleistung der einfachen Melderegisterauskunft (Art. 34 Abs. 1 MeldeG) ein automatisiertes Abrufverfahren über das Internet entwickelt. Wesentlicher Bestandteil ist dabei die elektronische Signatur und die Möglichkeit der anonymen Zahlung. Diese Anwendung soll in allen fünf beteiligten Städten (Bayreuth, Erlangen, Fürth, Nürnberg und Schwabach) des Städteverbundes Nürnberg zum Einsatz kommen.

Verfahrensbeschreibung

Die Anwendung ”Melderegisterauskunft” des MEDIA@Komm-Projektes der Region Nürnberg unterscheidet zwei Fallkonstellationen:

- Auskünfte an jedermann auf anonyme Anfrage mit Bezahlung der Gebühren per Geldkarte,
- Auskünfte auf Anfragen von Mitarbeitern registrierter privater Stellen (Firmen, Freiberufler usw.) mit Sammelabrechnung der Gebühren.

Personen der Fallgruppe 2 (Mitarbeiter registrierter privater Stellen) müssen sich bei der Anfrage durch die elektronische Signatur identifizieren (qualifiziertes Zertifikat eines angezeigten oder akkreditierten Zertifizierungsdiensteanbieters, starke Authentifizierung). Die Authentifizierung ist zum Nachweis der Kostenübernahmepflicht der registrierten privaten Stelle erforderlich.
Die Anfrage wird über bereitgestellte elektronische Formulare sowie entsprechende Hinweis- und Auswahlfenster gesteuert. Die Anfragedaten werden online mit den gespeicherten Daten bei der jeweiligen Meldebehörde abgeglichen und die Anfrage wird online beantwortet, wenn die Voraussetzungen des noch in Bayerisches Landesrecht umzusetzenden § 21 Abs. 1a Melderechtsrahmengesetz (MRRG) erfüllt sind.

Datenverarbeitung

Dienste – wie z.B. Signatur und Bezahlfunktion – werden für alle Städte zentral zur Verfügung gestellt, wobei die Datenhoheit der Kommunen gewährleistet ist, indem sämtliche zu speichernden und zu verarbeitenden Daten nur innerhalb der jeweiligen Kommune vorgehalten werden und keinerlei kommunenübergreifende Zugriffe möglich sind. Die Vertraulichkeit der Daten wird bei der Übertragung über das Internet durch SSL-Verschlüsselung mit 128 Bit oder andere Verschlüsselungsverfahren mit der gleichen Verschlüsselungsstärke gewährleistet.
Für die Authentifizierung mit Signaturkarte und für die Bezahlung mit der Geldkarte, werden signierte Java-Applets eingesetzt. Cookies werden (nur) eingesetzt, damit innerhalb einer Sitzung mehrere Auskünfte nacheinander eingeholt werden können. Cookies werden mit Beendigung der Sitzung aus dem Speicher des Nutzer-PC gelöscht. Das Verfahren funktioniert auch dann, wenn die Annahme von Cookies durch den Nutzer zurückgewiesen wird. Es sind damit lediglich Einbußen im Handhabungskomfort verbunden.
Es werden nur die Daten gespeichert, die benötigt werden, um die jeweilige Dienstleistung auszuführen und abzurechnen. Zugriffe auf Web-Server werden anonym protokolliert. Die Protokolle (Log-Dateien) werden für die Störungsanalyse und für anonyme statistische Auswertungen genutzt und nach 30 Tagen gelöscht. Protokollein-

tragungen, die für den Nachweis und die Durchsetzung von Zahlungsansprüchen benötigt werden, werden spätestens 180 Tage nach vollständiger Zahlung gelöscht.
Ein noch zu klärender Aspekt ist u.a. die technische Realisierung des im geänderten MRRG geregelten Widerspruchsrechts gegen eine Meldeauskunft über das Internet.

Datenschutzrechtliche Bewertung:

Das Verfahren nutzt die derzeit verfügbaren technischen Möglichkeiten zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der über Internet übertragenen Daten. Dabei wird auch darauf geachtet, die Datenerhebung und Dauer der Datenspeicherung auf das erforderliche Maß zu begrenzen.
Der praktische Einsatz im Echtbetrieb ist jedoch erst möglich, wenn § 21 Abs. 1a Melderechtsrahmengesetz (MRRG) in das Bayerische Meldegesetz umgesetzt ist. Dies ist im Gesetzentwurf für das "Gesetz zur Stärkung elektronischer Verwaltungstätigkeit" vorgesehen. Das Gesetz soll zum 01.01.2003 in Kraft treten.

Projektbetreiber:
Curiavant Internet GmbH, Hauptmarkt 17, 90403 Nürnberg
E-Mail: info@curiavant.de

für die Städte Bayreuth, Erlangen, Fürth, Nürnberg und Schwabach

7.2.16 Ratsinformationssystem der Stadt Norderstedt

Der Einstieg in die Info-Datenbank erfolgt von der Homepage der Stadt Norderstedt aus unter dem Stichwort Ratsinformationssystem. Es enthält neben allgemeinen Angaben über die politischen Gremien der Stadt in einem besonders abgeschotteten Bereich sämtliche Sitzungsvorlagen, Einladungen und Auszüge aus den Niederschriften über die öffentlichen Sitzungen der Stadtvertretung und ihrer Ausschüsse. Die Pflege der Datenbank erfolgt seit dem Jahr 1998. Allerdings sind insbesondere in den Sitzungsvorlagen auch Daten über die jeweils zuständigen Mitarbeiter enthalten. Während für die Veröffentlichung personenbezogener Daten der Mandatsträger in den Angaben über die politischen Gremien der Stadt noch die Einwilligung der Betroffenen eingeholt werden konnte, war dies bei den Beschäftigten schon allein im Hinblick auf die Vielzahl der Mitarbeiter der Stadt nicht praktikabel. Man musste sich deshalb nach einer anderen Lösung umsehen. Aus datenschutzrechtlicher Sicht ist eine Veröffentlichung von Mitarbeiterdaten im Internet dann bedenklich, wenn diese Daten über Internetsuchmaschinen mit anderen Daten der Betroffenen in Verbindung gebracht werden können. So können z. B. Informationen über die dienstliche Stellung ohne weiteres mit Daten aus dem privaten Bereich verknüpft werden. Die Gefahr liegt nicht fern, dass aus dieser Zusammenführbarkeit Ansätze eines Persönlichkeitsprofils der Betroffenen entstehen können. Potentielle Arbeitgeber, Vermieter oder andere Interessierte könnten sich so eine Vielzahl von Informationen über die Betroffenen beschaffen. Um der dargestellten Gefahr in der gebotenen Weise zu begegnen, stehen dem Internetnutzer die in dem besonders abgeschotteten Teil der Datenbank enthaltenen Informationen erst zu Verfügung, wenn eine entsprechende Datenbankabfrage durch manuelle Eingabe eines oder mehrerer Suchbegriffe gestartet wird. Eine direkte Verlinkung auf die Sitzungsunterlagen von anderen Seiten der Homepage besteht nicht. Dies schützt die Dokumente sicher vor einer Indizierung durch Internetsuchmaschinen. Die datenschutzrechtlichen Bedenken gegen eine Bereitstellung von Mitarbeiterdaten im Internet sind damit ausgeräumt.

Datenschutzrechtliche Bewertung:

Die Stadt Norderstedt betreibt über ihre Homepage eine Info-Datenbank, in der u. a. auch Mitarbeiterdaten dem Internetnutzer zur Verfügung gestellt werden. Durch eine Beschränkung der Recherchemöglichkeiten - der Zugriff ist ausschließlich über eine durch Suchbegriffe veranlasste Datenbankabfrage möglich - werden die Daten allerdings wirksam vor einer Indizierung durch Internetsuchmaschinen geschützt. Die Gefahr einer Verknüpfung der Daten mit anderen Datenbeständen kann so ausgeschlossen werden. Unter dieser Voraussetzung ist eine Bereitstellung von Mitarbeiterdaten im Internet auch aus datenschutzrechtlicher Sicht unbedenklich.

Projektbetreiber:

Stadt Norderstedt, Rathausallee 50, 22486 Norderstedt
eMail: edv@norderstedt.de

7.2.17 Ratssitzungen im Internet in Düsseldorf

Die Bezirksregierung Düsseldorf hat für die Sitzungen des Regionalrates ein Online-Verfahren entwickelt, das seit mehreren Jahren fester Bestandteil ihres Serviceangebotes ist. Kernstück ist die Übertragung der laufenden Sitzungen des Regionalrates per Videostream ins Internet. Flankierend dazu können als Begleitservice Beratungsunterlagen heruntergeladen werden. Das Verfahren erfreut sich auch bei anderen Behörden bereits großer Nachfrage.

Speicherung von erhobenen Daten / Löschung

Erhoben werden sowohl das gesprochene Wort als auch das Bild von den Delegierten – also den von den Kommunalparlamenten entsandten Mandatsträgern – und auch von den an der Versammlung als Vertreter der Fachbehörden teilnehmenden Verwaltungsmitarbeitern der Bezirksregierung Düsseldorf oder am jeweiligen Verfahren fachlich beteiligten sonstigen Behörden. Daneben kann auch die Zuhörerschaft im Rahmen der Versammlung mit aufgenommen werden. Diese Daten (Filmaufnahmen in Ton und Bild) werden neben den Sitzungsunterlagen gespeichert, um im Bedarfsfall von den interessierten Nutzerinnen und Nutzern abgerufen zu werden. Gelöscht werden sie in Abhängigkeit von der Nachfrage serviceorientiert.

Zielgruppen

des Webcasting und des Begleitservice sind die interessierte Öffentlichkeit, Bürgerinnen und Bürger, die Mitglieder des Regionalrates und der Kommunalparlamente selbst, die Medien, gesellschaftliche Gruppen, Schulen, Investoren und auch die Beschäftigten der (Landes-)Verwaltung mit dem Bedürfnis an zeitnaher Anteilnahme an raumbedeutsamen Planungsentscheidungen des Regionalrates.

Legitimation durch Verfahren

Die Sitzungen des Regionalrates sind öffentlich (§ 8 Abs. 3 LPlG). Damit ist neben der Sitzungsöffentlichkeit, also der ungehinderten Zugangsmöglichkeit für jedermann nach Maßgabe der vorhandenen Raumkapazitäten, auch die Berichterstattungsöffentlichkeit gewährleistet. Dies beinhaltet die Zugangsmöglichkeiten für die Medien – Presse, Rundfunk, Fernsehen und auch Internet. Hier wird die Öffentlichkeit als elementares Prinzip der Demokratie und des Rechtsstaats im Interesse von Transparenz und vertrauensbildender Maßnahme in den vom Regionalrat betriebenen Verfahren fixiert. Daneben steht die Serviceorientierung, zeitnahe und papiersparende Informationsbereitstellung auch über den Tag der Sitzung hinaus. Zur Information aller Beteiligten muss vor Beginn der Übertragung auf diese hingewiesen werden.

Datenschutzrechtliche Bewertung:

Das Verfahren ist in Übereinstimmung mit den datenschutzrechtlichen Regelungen und den Bestimmungen des seit dem 01.01.2002 in Kraft getretenen Informationsfreiheitsgesetzes und des Rechts am eigenen Bild implementiert worden. Die Sitzungen des Regionalrates sind grundsätzlich öffentlich. Damit ist die Zulassung von Presse, Rundfunk, Fernsehen und auch Internet sichergestellt. Die aufgenommenen Daten sind damit allgemein zugänglich.

Projektbetreiber:

Bezirksregierung Düsseldorf
Cecilienallee 2
40474 Düsseldorf
www.bezreg-duesseldorf.nrw.de.
robin.weiss@brd.nrw.de

7.2.18 Sperrgutabholung in Bayreuth

Die Online-Anwendung Sperrgutabholung Stadt Bayreuth (Anzeige) ist im Produktiveinsatz. Bisher wurde dies über ein weitgehend formloses schriftliches oder telefonisches Verfahren abgewickelt.

Verfahrensbeschreibung

Über Online-Formulare werden personen- und fachspezifische Daten (Pflichtangaben und freiwillige Angaben) erhoben. Erklärungen und Hinweise werden ebenfalls im Rahmen der Online-Formulare gegeben. Eine besondere Authentifizierung oder eine elektronische Signatur sind nicht erforderlich, da auch heute bereits diese Anträge bzw. Anzeigen telefonisch möglich sind. In beiden Verfahren werden mit Antrag/Anzeige auch keine unmittelbaren Gebühren wirksam.
Der Einstieg erfolgt über eine Seite mit Informationen zum Thema Sperrgutabholung. Aus dieser Einstiegsseite wird verlinkt auf:

- Erläuterungen der Dienststelle,
- Datenschutzhinweise.

Datenverarbeitung

Die Daten werden in der Online-Anwendung auf Vollständigkeit geprüft und strukturiert zusammengestellt. Die Verbindung zum Webserver wird grundsätzlich SSL-verschlüsselt (128 Bit, SSL-Zertifikat). Es werden nur die für die Sachbearbeitung erforderlichen Daten erhoben. Die Abgabe von Erklärungen bzw. die Bestätigung einer Kenntnisnahme von Hinweisen wird durch aktives Anklicken von Checkboxen realisiert. Werden diese Bestätigungen nicht abgegeben, werden entsprechende Fehler- bzw. Hinweismeldungen von der Anwendung ausgegeben und der Online-Vorgang kann nicht abgeschlossen werden. Sind alle Daten vollständig, werden diese in einer Übersicht, die zusätzlich auch in druckfreundlichem Format angeboten wird, zusammengestellt und können vom Nutzer nochmals überprüft und ggf. korrigiert werden. Die Daten werden per eMail an eine definierte Adresse der Dienststelle verschickt. Die Verbindung zum Mailserver der Kommune erfolgt direkt über Glasfaserkabel. Die Datenspeicherungen sind auf ein Jahr begrenzt.

Datenschutzrechtliche Bewertung:

Das Verfahren nutzt die derzeit verfügbaren technischen Möglichkeiten zur Sicherstellung von Vertraulichkeit und Integrität der über Internet übertragenen Daten. Maßnahmen zur Sicherstellung der Authentizität sind nicht erforderlich. Das Verfahren zeigt überdies Möglichkeiten zur Umsetzung der Forderungen des Teledienstedatenschutzgesetzes (TDDSG) auf.

Projektbetreiber:

Curiavant Internet GmbH, Hauptmarkt 17, 90403 Nürnberg
eMail: info@curiavant.de
für die Städte Bayreuth, Erlangen, Fürth, Nürnberg und Schwabach.

7.2.19 Steuererklärung (ELSTER)

Mit dem Projekt ELSTER soll Steuerpflichtigen und Steuerberatern die Möglichkeit eröffnet werden, Steuererklärungen in elektronischer Form zu erstellen und dem zuständigen Finanzamt per Datenfernübertragung zu übermitteln. ELSTER wurde von der IT-Stelle der Oberfinanzdirektion München entwickelt und wird bundesweit eingesetzt. Um ELSTER möglichst einfach in bereits vorhandene Finanz-Softwarepakete verschiedener Anbieter zu integrieren, hat die IT-Stelle der Oberfinanzdirektion München den Softwarebaustein "Telemodul" entwickelt und für den bundesweiten Einsatz freigegeben. Daneben stellt die Steuerverwaltung mittlerweile auf dem entsprechenden Server auch ein Einkommersteuerprogramm für Bürger kostenlos zum Download zur Verfügung. Zurzeit muss parallel zu den elektronischen Daten noch eine sog. Komprimierte Steuererklärung in Papierform übermittelt werden (siehe ”Verfahrensbeschreibung”). Demnächst wird dies nicht mehr nötig sein. Das ELSTER-Verfahren wird fortlaufend auf alle steuerlich relevanten Daten ausgedehnt. Zu den bereits realisierten Bereichen zur Übermittlung von Jahressteuererklärungsdaten (Einkommensteuer, Umsatzsteuer, Gewerbesteuer), Lohnsteueranmeldungen und Umsatzsteuer-Voranmeldungen und der Bereitstellung von Einkommensteuerbescheiddaten ist geplant, das Verfahren auf weitere Steuerarten und die Einbeziehung von Steuerbescheinigungen (Kapitalertragsteuern, Vermögenswirksame Leistungen etc.) sowie notwendige Anlagen (Bilanzen, GuV-Rechnung) auszuweiten. Dabei wird die so genannte "Elektronische Lohnsteuerkarte" vordringlich realisiert. Dann kann der Arbeitgeber die entsprechenden Daten direkt an das Finanzamt leiten. Ein weiterer zentraler Punkt ist die Schaffung von Online-Diensten über das Internet. Vorgesehen sind hier die Möglichkeiten der Online-Steuerkontoabfrage und die Abfrage des Bearbeitungsstandes der Steuererklärung.

Rechtliche Grundlagen

Die Abgabenordnung sieht in § 150 Abs. 6 AO auch die Möglichkeit vor, dass Steuererklärungen oder sonstige für das Besteuerungsverfahren erforderliche Daten ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermittelt werden können. Ein derartiges Verfahren ist aber an den Erlass einer entsprechenden Rechtsverordnung gebunden. Für die künftig mögliche rein elektronische Steuererklärung wird mit der Steuerdaten-Übermittlungsverordnung die erforderliche Rechtsgrundlage geschaffen.

Verfahrensbeschreibung

Der Ablauf stellt sich bei Verwendung einer handelsüblichen Finanzsoftware wie folgt dar: Steuerpflichtige erstellen zunächst ihre Steuererklärung mit Hilfe der handelsüblichen Finanzsoftware auf dem eigenen PC. Nachdem alle Eingaben von dieser Software auf Plausibilität geprüft wurden, werden die Steuerklärungsdaten verschlüsselt und signiert und sodann über das Internet an einen Server der IT-Stelle der Oberfinanzdirektion München der bayerischen Steuerverwaltung oder alternativ des Rechenzentrums der Finanzen in Düsseldorf (so genannte Clearingstelle) gesendet. Die Clearingstelle ordnet die empfangenen Daten dem jeweiligen Bundesland zu und stellt sie den Finanzverwaltungen auf einem weiteren Server zum Abruf bereit. Nach dem Abruf durch das jeweilige Bundesland mit einem speziellen Programm (Elster

Control Center – ECC) werden die Daten entschlüsselt, geprüft und für die weitere Verarbeitung im jeweiligen Steuerrechenzentrum umgesetzt. Die Daten durchlaufen die Festsetzungsprogramme dann wie die aus den Finanzämtern auf konventionellem Weg transferierten Daten. Parallel zum elektronischen Weg muss der Steuerpflichtige zurzeit noch die Kurzform seiner Steuererklärung, die sog. Komprimierte Steuererklärung, am eigenen PC ausdrucken, handschriftlich unterschreiben und dem zuständigen Finanzamt zusenden. Das Finanzamt beginnt mit der Bearbeitung nur, wenn die auf der Komprimierten Steuererklärung vermerkte Telenummer mit der der elektronisch übermittelten Daten übereinstimmt.

Datenschutzrechtliche Bewertung:

Bei der Verarbeitung von Steuerdaten werden besonders hohe Ansprüche an Vertraulichkeit und Integrität der Daten gestellt, um das in § 30 AO normierte Steuergeheimnis zu wahren. ELSTER erfüllt diese Anforderung in angemessener Weise. Um die Vertraulichkeit und Integrität der elektronisch übermittelten Steuerdaten zu gewährleisten, werden die anerkannten kryptografischen Algorithmen Triple-DES und RSA genutzt. Die Steuerverwaltungen der Länder erzeugen das Schlüsselpaar (geheimer und öffentlicher Schlüssel) für den RSA-Algorithmus selbst. Das hierfür entwickelte vertrauenswürdige Verfahren stellt sicher, dass der geheime Schlüssel, der zur Entschlüsselung der übermittelten Steuerdaten erforderlich ist, ausschließlich den zuständigen Stellen der Finanzverwaltung zugänglich ist. Der öffentliche Schlüssel wird an die IT-Stelle der Oberfinanzdirektion München auf einem besonders gesicherten Weg übermittelt und in das Telemodul eingebunden. Somit steht er jedem Steuerpflichtigen zur Verschlüsselung seiner Daten zur Verfügung.

Projektbetreiber

Oberfinanzdirektion München, - IT-Bereich -, Meiserstraße 8, 80333 München;
eMail: elsterhotline@elster.de;
Fax: 089/5995-8008
für die deutsche Steuerverwaltung

7.2.20 Strafanzeige der Polizei Köln

Die Polizei Köln bietet seit April 2000 die Möglichkeit, über das Interent vom heimischen oder betrieblichen PC aus Online-Anzeigen einzureichen. In vielen Fällen kann jedoch der persönliche Kontakt der anzeigenden Person nicht vollständig durch den PC ersetzt werden. Der erste Kontakt zur Polizei kann damit aus der Distanz ohne den z.T. aufwändigen Weg zur Dienststelle in Ruhe am eigenen häuslichen Schreibtisch (oder auch über den Internetzugang am Arbeitsplatz) erfolgen. In Eilfällen sollte der Notruf der Polizei genutzt werden. In Fällen, in denen nicht der unmittelbare telefonische Kontakt mit der Polizei erforderlich scheint, kann von der betroffenen Person oder einem Dritten eine Anzeige online erstattet werden. Das im Internet angebotene Formular bietet bereits eine Palette von bestimmten Delikten (Diebstahl, Körperverletzung, Straßenverkehr, Internet oder sonstige Delikte als Vorauswahl) an, sodass das Anzeigeformular dem Delikt angepasst und somit einfacher für den Bürger auszufüllen ist. Nach Ausfüllen des Formulars werden alle Einträge auf einer Bestätigungsseite angezeigt, diese kann für die persönlichen Unterlagen ausgedruckt werden. Anschließend erfolgt die Übertragung per verschlüsselter eMail, die zentral abgerufen, zugeordnet und weitergeleitet werden. Der Sachbearbeiter wird dann im Bedarfsfall auf den Anzeigenden telefonisch oder schriftlich zukommen. Die örtliche Zuständigkeit der Polizei richtet sich nach dem Ort, an dem die Tat begangen worden ist, dem Tatort. Soweit dieser nicht im Bereich der Polizei Köln liegt, wird die Anzeige an die örtlich zuständige Polizeidienststelle weitergeleitet und der oder die Anzeigende entsprechend informiert.
Im Formular werden die Personalien der anzeigenden Person (Name, Geschlecht, Geburtsdatum, -ort, Wohnort, Telefon), die Beschreibung des Tatort und Angaben zur Tatzeit, zu Tatverdächtigen und Zeugen mit Name und Anschrift und eine Sachverhaltsbeschreibung abgefragt. Automatisiert wird die IP-Adresse mit übertragen. Auf dem eMail-Server werden die eingegangenen eMails zur Mißbrauchskontrolle maximal ein Jahr geseichert.

Datenschutzrechtliche Bewertung:

Das Verfahren wurde unter Beachtung der datenschutzrechtlichen Regelungen erstellt. Der Zugang erfolgt via Internet über eine sichere Verbindung mit der Möglichkeit der Serveridentifikation (SSL-Verschlüsselung mit Serverzertifikat, das beim LDS als Zertifizierungsinstanz hinterlegt ist). Die Anzeige kann per angebotenem Formular übersandt werden. Aber auch eine Anzeige per eMail über eine PGP-Verschlüsselung ist möglich. Dazu kann kostenlos der Verschlüsselungscode für das Programm PGP von der Nutzerin oder dem Nutzer von der Website der Polizei heruntergeladen werden. Die Eingangsbestätigung erfolgt über eMail, wenn eine gültige eMail-Adresse angegeben wurde.

Projektbetreiber:

Polizeipräsidium Köln
Walter-Pauli-Ring 2-4
51103 Köln
www.polizei.nrw.de/koeln, **www.polizei-koeln.de**;
webmaster@mail.pp-koeln.nrw.de, **info@polizei-koeln.de**

7.2.21 Verfahrensverzeichnis und Vorabkontrolle in Duisburg

Gem. § 8 DSG NRW ist jede verantwortliche Stelle verpflichtet, automatisierte Verfahren zu beschreiben. Gem. § 10 Abs. 3 DSG NRW ist eine Vorabkontrolle durchzuführen. Die Zuständigkeit zur Zusammenführung der einzelnen Verfahren zu einem Verfahrensverzeichnis und für die Durchführung der Vorabkontrolle als Bestandteil des Sicherheitskonzeptes liegt beim Datenschutzbeauftragten (§ 32 a Abs. 1, S. 6, Abs. 3, S. 2 DSG NRW). Zur Erarbeitung eines Verzeichnisses aller aktuellen Anwendungen/Verfahren und zur Durchführung der Vorabkontrolle hat die Stadt Duisburg ein DV-gestütztes automatisiertes Verfahren erarbeitet. Die Verfahrensbeschreibung wird standardisiert über eine vorgegebene Maske von dem jeweils zuständigen Fachbereich ausgefüllt und per eMail der Stabsstelle Datenschutz übermittelt. Fußend auf dieser Beschreibung führt der Datenschutzbeauftragte die erforderliche Vorabkontrolle am Bildschirm per Einzelentscheidung durch (Vergabe von Bewertungspunkten und Entscheidung über Summenbildung). Das Ergebnis der Vorabkontrolle wird zusammengefasst und den Fachbereichen übermittelt.
Das Verfahren wird, soweit es rechtlich zulässig ist, vollständig elektronisch verwaltungsintern abgebildet bei Beteiligung der Fachämter und des Datenschutzbeauftragten. Die Daten werden verschlüsselt übertragen und erfüllen somit die Vertraulichkeitsanforderungen der datenschutzrechtlichen Reglungen. Halbautomatisch erfolgt die Vorabprüfung, da hier die individuelle Einzelfallbewertung der Sensibilität der Daten durch den Datenschutzbeauftragten erforderlich ist und nicht automatisch vom PC übernommen werden kann. Grundlagen für die individuelle Einzelfallbewertung sind die Merkmale Vertraulichkeit, Integrität und Verfügbarkeit i.V.m. der Schutzstufenzuordnung (A-E nach BSI). Auch Informationsbegehren von Bürgerinnen und Bürgern werden im Einzelfall entschieden, sodass der Schutz der im Verzeichnis niedergelegten personenbezogenen Daten durch den Datenschutzbeauftragten sichergestellt wird.
Das Verfahren kann über das Medium CD auch für andere verantwortliche Stellen bereitgestellt werden. Niedergelegt sind Verfahrensbeschreibung und teilautomatisierte Vorabkontrolle, Informationen zur Installation und Anwendung, DSG NRW, Beschreibung der Maßnahmen des BSI-Grundschutzhandbuches versehen mit einem Link.

Datenschutzrechtliche Bewertung:

Das Verfahren ist in Übereinstimmung mit den datenschutzrechtlichen Regelungen erstellt worden. Die personenbezogenen Daten werden über eine sichere Verbindung per eMail verschlüsselt vom Fachamt an die Stabsstelle für Datenschutz übermittelt.
Der Zugang der Bürger auf dieses Verzeichnis wird durch Einzelanfrage unter Beachtung des Schutzes der im Verzeichnis vorhandenen personenbezogenen Daten von der Stabsstelle sichergestellt.

Projektbetreiberin:

Die Oberbürgermeisterin der Stadt Duisburg
Memelstraße 25 – 33
47049 Duisburg
www.duisburg.de; **Saupe@stadt-duisburg.de**

7.2.22 Videokonferenz bei der Bezirksregierung Düsseldorf

- Telekooperation in der Vermessungsverwaltung (Projekt “Teams”) -

Hintergrundverfahren in der Vermessungsverwaltung

Die Bezirksregierung Düsseldorf hat zusammen mit dem Institut für Arbeit und Technik im Wissenschaftszentrum NRW das Projekt “Teams” ins Leben gerufen, das über Videokonferenzen und Application-Sharing die Ablösung der analogen Liegenschaftskarte und des analogen Liegenschaftsbuchs durch die digitalen Datenbestände der Automatisierten Liegenschaftskarte (ALK) und des Automatisierten Liegenschaftsbuches (ALB) zum Gegenstand hat. Im Liegenschaftsbuch sind mit dem Grundbuch abgeglichene personenbezogene Daten (Grundstück und Eigentümer) nachrichtlich enthalten, die zusammen mit den Daten der Liegenschaftskarte (Flur, Flurstück, Flurstücksnummer, Lage und Geometrie) präzise den “Gegenstand” eines im Grundbuch verankerten persönlichen Eigentumsrechts beschreiben. Das Liegenschaftskataster (ALK und ALB) wird bei den Katasterämtern der Kreise und kreisfreien Städte geführt und steht jedermann zur Einsichtnahme offen, soweit er ein berechtigtes Interesse darlegt. Zusammen mit dem Amtlichen Topographisch-Kartographischen Informationssystem (ATKIS) beim Landesvermessungsamt, das Flächen gleicher Nutzung ausweist, steht eine umfassende und flexible Datengrundlage für alle Anwendungen der Geoinformation zur Verfügung.

Videokonferenzen und Application-Sharing

Die am Projekt teilnehmenden Städte Mülheim an der Ruhr, Oberhausen und der Kreis Neuss (Katasterämter) haben die erforderlichen Daten erfasst. Die Bezirksregierung Düsseldorf hatte sie nach Abschluss der Erfassung zu prüfen und zu genehmigen. Im Zuge der Erstellung der Karten fanden prozessbegleitend intensive Beratungen zwischen der Bezirksregierung und den Katasterämtern statt, die der Qualitätssicherung und Vereinheitlichung dienten. Die Organisation dieses Arbeits- und Prüfprozessen wurde ständig weiterentwickelt und mündete 1997 in das Projekt “Teams”, in dem ein online-basiertes Application-Sharing in Verbindung mit audiovisueller Kommunikation erprobt und entwickelt worden ist. Das Projekt sollte die erforderlichen technischen Voraussetzungen schaffen und die mit dem Verfahren verbundene Organisationsentwicklung unterstützen. Eine spätere Übertragbarkeit der Erfahrungen auf andere Bezirksregierungen, Katasterämter oder sonstige Nutzer sollte eruiert werden. Nach Abschluss letzter technischer Tests im März 1998 wurde das Projekt gemeinsam mit der Stadt Mülheim an der Ruhr anhand von praktischen Anwendungen der Öffentlichkeit vorgestellt. Das Projekt hatte eine Laufzeit von 2 Jahren und wurde im Okt. 1999 abgeschlossen.

Zielgruppen

Zielgruppe der Videokonferenz und des Application-Sharing sind die beteiligten Behörden (Katasterämter der Städte Mülheim a.d.R., Oberhausen und der Kreis Neuss und die Bezirksregierung Düsseldorf). ALB und ALK (und auch ATKIS) dagegen werden genutzt von landesweit 54 Katasterämtern sowie von Bürgern, Architekten, Bauherren und Käufern mit berechtigtem Interesse.

Ergebnis des Projekts

Nach Abschluss des Projekts wurde nach Aussage aller Anwender dessen Durchführung als ausgesprochen erfolgreich bewertet. Videokonferenz und Application-Sharing haben eindeutige Beschleunigungs-, Synergie-, Anschaulichkeits-, Öffnungs- und Vertrauenseffekte. Umständliche und (kosten-)aufwändige Dienstreisen entfallen, direkte gemeinsam diskutierte Entscheidungsfindung, schnelle, standortübergreifende Kooperation wird gefördert. Der Nutzen übersteigt schnell den Aufwand durch erhebliche Produktivitätssteigerung.

Datenschutzrechtliche Bewertung

Das Verfahren ist in Übereinstimmung mit den datenschutzrechtlichen Regelungen durchgeführt worden. Die über die Videokonferenz erhobenen Daten sind nur den Teilnehmern zugänglich, werden nicht gespeichert und nach Ende der Konferenz sind Wort und Bild gelöscht. Die über die ALK und das ALB erhobenen Daten werden ständig aktualisiert und damit entsprechend den tatsächlichen Veränderungen angepasst. Der Zugriff der Nutzer mit berechtigtem Interesse erfolgt nach Einzelfallentscheidung.

Projektbetreiber:

Bezirksregierung Düsseldorf
Cecilienallee 2, 40474 Düsseldorf
www.bezreg-duesseldorf.nrw.de; **michael.vedder@brd.nrw.de**

7.2.23 Virtuelles Rathaus der Stadt Hagen

Die Weiterentwicklung der Bürgerämter mit zukunftsorientierten IT-Technologien und elektronischen Kommunikationsformen wird zzt. im Virtuellen Rathaus Hagen realisiert, mit den Bürgerinnen und Bürgern erprobt und fortentwickelt. Die Kooperationspartner Feruniversität Hagen, die i-World GmbH und die Stadt Hagen (HABIT), Hagener Betrieb für Informations-technologie entwickelten dieses Onlineprojekt. Ziel des Virtuellen Rathauses ist es, den Weg der Bürgerinnen und Bürger zur Verwaltung so einfach, so bequem und so verständlich wie nur möglich zu gestalten, oder mit anderen Worten: „Die bürgerleichtere Verwaltung“ anzubieten. Auch die Möglichkeiten der Rückkoppelung von Bürgerwünschen sollen so erleichtert werden.

Leistungen für Bürgerinnen und Bürger

Neben Verwaltungsinformationen zu allen städtischen Dienstleistungen, Formularen und städtischen Rechtsvorschriften können Dienstleistungen der Stadtverwaltung von der Wunschkennzeichen-Reservierung über die einfache Melderegisterauskunft bis zur aktuellen Liegenschaftsauskunft online abwickelt werden. Dieses Angebot wird Zug um Zug weiter ausgebaut, sodass in Zukunft jede Anfrage schnell und in wenigen Schritten zum entsprechenden Leistungsangebot führt. Bei Bedarf wird der Bürger durch Hilfefunktionen unterstützt und geleitet. Das System nutzt bestehende kommunale DV-Anwendungen und gibt einen Rahmen für Erweiterungen und den Anschluss neuer kommunaler IT-Fachverfahren. Beispiele sind das Versenden und Empfangen von eMails, die Nutzung von Online-Datenbanken und der elektronische Datenaustausch von Dokumenten und Vorgängen.
Ein Online-Bezahlverfahren ist ebenfalls realisiert.

Übertragbarkeit und Anpassungsfähigkeit

Als Fundament für das Virtuelle Rathaus steht eine technische Plattform zu Verfügung, die sowohl funktional als auch technologisch die Anpassung, Erweiterbarkeit und Übertragbarkeit in andere Umgebungen ermöglicht. Es wurde eine offene und skalierbare Lösung geschaffen, die auf andere Kommunalverwaltungen - unabhängig von der dort vorherrschenden technischen Plattform - übertragen werden kann.

Datenschutzrechtliche Bewertung:

Dem Bedürfnis und der Notwendigkeit nach Datenschutz und Datensicherheit wird insbesondere in den folgenden Punkten Rechnung getragen:
An den Schnittstellen zwischen dem öffentlichen (weltweiten) Internet und dem geschlossenen (verwaltungsinternen) Intranet sind zu diesem Zweck geeignete Sicherheitsmaßnahmen realisiert. Kernpunkte des Sicherheitskonzeptes sind:

- Firewallsystem im Form eines Screened Subnets (Zugriffsschutz) mit dezidierten Sicherheits-Policies
- Authentizitäts-Prüfung der Kommunikationspartner durch den Einsatz der qualifizierten elektronischen Signatur (Echtheitsnachweis) bei Zugriff auf kommunale, personenbezogene Datenbestände. Die qualifizierte elektronische Signatur der Signtrust ist im Betrieb. Die Signatur der Telesec wird derzeit in das System eingebaut. In den Zugriffsfällen, in denen die qualifizierte elektronische Signatur nicht ausreicht, wie zum Beispiel beim Nachweis des berechtigten Interesses für den Zugriff auf das Liegenschaftskatasterkartenwerk oder das Liegenschaftsbuch, wird zusätzlich eine Registrierungsdatei mit den Signaturschlüssel-Informationen der qualifizierten elektronischen Signatur eingesetzt.
- Vertraulichkeit und Integrität (Unverfälschtheit) durch Verschlüsselung des personenbezogenen Datenverkehrs mittels HTTPS (128 BIT-Verschlüsselung).
- Die Beachtung der datenschutzrechtlichen Rahmenbedingungen wie Anbieterkennzeichnung, die Anzeige der Weitervermittlung auf andere externe Anbieterinnen und Anbieter durch geeignete Hinweise, Informationen zum Datenschutz und eine Standardverschlüsselung ist selbstverständlich.

Projektbetreiber:

Stadt Hagen
HABIT
Hagener Betrieb für Informationstechnologie

Erstellt von: HABIT, Peter Klinger, Peter.Klinger@stadt-hagen.de

7.2.24 Volkshochschule in Duisburg

Mit der Website der VHS bietet die Stadt Duisburg ihren Bürgerinnen und Bürgern einen umfassenden Überblick über das Angebot der VHS. Auf kurzem Wege und unabhängig von Öffnungszeiten und Warteschlangen können hier schnell und unbürokratisch das Angebot eingesehen werden, Änderungen zur Kenntnis genommen, Anmeldungen durchgeführt und bezahlt werden. Die Internetpräsenz der VHS der Stadt Duisburg ist sowohl über das Portal der Stadtverwaltung Duisburg (URL: www.duisburg.de) als auch über die URL www.vhs-duisburg.de erreichbar.

Internes Verfahren

Die Anwendung „V2000“ arbeitet mit einer INFORMIX-Datenbank auf einem UNIX-Betriebssystem und bietet in einem geschlossenen und autonomen Netzwerk folgende Nutzungsmöglichkeiten:
Kursdateneingabe: Veranstaltungsplanung, Veröffentlichung, Anmeldung,
Teilnehmerdateneingabe: Anmeldung, Gebühreneinzug,
Kursleiterdateneingabe: Einsatzplanung, Honorarabrechnung,
Schnittstelle zur Übermittlung von notwendigen Kursdaten ins Internet im gleichen Umfang wie in der Druckausgabe des VHS-Programms.

Der Zugang zu dieser Anwendung erfolgt über eine Emulation auf den Clients an den Arbeitsplätzen. Ein abgestuftes Zugriffsberechtigungssystem ermöglicht dem/der hauptberuflichen VHS-Mitarbeiter/-in nach Eingabe des Logins und eines geheimen Kennwortes die Bearbeitung der Daten.

Internetangebot

Allgemeine und aktuelle Informationen wie z.B. Öffnungszeiten, Anmeldebedingungen oder auch die Bekanntgabe von Kursausfällen per Newsticker werden angeboten. Eine Seite mit einer sich automatisch aktualisierenden 14-Tage-Vorschau für Einzelveranstaltungen ist eingestellt. Buttons für Sonderveranstaltungen und Projekte oder zu VHS-eigenen Unterportalen wie z.B. die „duisburger filmwoche“ oder das „FILMFORUM“ können bedient werden. Links zu ausgewählten Bildungsportalen der Erwachsenenbildung und zu weiteren Bildungsbereichen sind implementiert. Die Daten werden ständig gepflegt und auf dem Web-Server bereitgestellt.
Abfragemöglichkeiten von Veranstaltungsdaten des aktuellen Semesters bestehen für jedermann auf anonyme Anfrage in einfacher und erweiterter Form (auch Volltextsuche). Es werden die allgemeinen Veranstaltungsdaten einschließlich Belegungsstatus gezeigt. Einblicke in Teilnehmerlisten sind nicht möglich. Die aktualisierten Veranstaltungsdaten werden 1-mal täglich vom internen VHS-Server auf den Web-Server übertragen.
Eine Online-Anmeldung ist ebenfalls möglich. Die Eingabe der persönlichen Daten wie Name, Vorname, Adresse (kein Geburtsdatum!) erfolgt verschlüsselt (128-Bit-SSL) und ist somit gegen Einsicht durch Dritte geschützt. Soll die Bezahlung initiiert werden, kann eine Bankverbindung im Falle einer erteilten Einzugsermächtigung angegeben werden. Die Anmeldewünsche werden durch Übermittlung der eingegebenen Daten per Mail vom Web-Server an den/die entsprechenden Mitarbeiter/-innen in

der VHS weitergeleitet. In der VHS werden sie weiter bearbeitet und, wie für jede/n anderen Teilnehmer/-in auch, postalisch bestätigt.

Datenschutzrechtliche Bewertung:

Es werden die für die Anmeldung, Durchführung und Abrechnung von Kursen erforderlichen Daten erhoben und gespeichert. Die Daten werden nur für den Zweck verarbeitet, für den sie erhoben worden sind. Eine Verwendung erfolgt nicht für andere (dienstliche) Zwecke und eine Weitergabe an andere Behörden oder Firmen und Personen erfolgt dann, wenn dafür eine gesetzliche Grundlage besteht oder eine Einwilligung vorliegt. Der Zeitraum der Speicherung richtet sich nach den bestehenden gesetzlichen Vorschriften.

Projektbetreiber:

Volkshochschule der Stadt Duisburg
Am König-Heinrich-Platz
47049 Duisburg
www.duisburg.de; a.rehrmann@stadt-duisburg.de

7.3 Media@Komm-Projekte

Die Präsenz von Städten und Gemeinden im Internet wächst. Der breite Durchbruch zur rechtsverbindlichen Interaktion in elektronischen Netzen auf Basis der elektronischen Signatur steht noch aus. Hier setzt das Projekt MEDIA@Komm an, welches eingegliedert in das Aktionsprogramm „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts“, durch das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF), als eine der größten deutschen Initiativen zur Entwicklung und Umsetzung von Multimediaprojekten in Städten und Gemeinden ins Leben gerufen wurde. In einem Förderwettbewerb wurden die Städte und Gemeinden ermittelt, welche die besten integrativen Konzepte zur Entwicklung von multimedialen Diensten, möglichst unter Nutzung der elektronischen Signatur, entwickelt haben. Unter Weiterführung des Bundesministeriums für Wirtschaft und Arbeit (BMWA) wurden insgesamt fast € 25 Millionen an Fördermitteln investiert, etwa die gleiche Summe floss zusätzlich durch Investoren der Privatwirtschaft in das Projekt.

Am Wettbewerb beteiligten sich 136 Städte und Gemeinden. Preisträger wurden die Stadt Esslingen, die Region Nürnberg/Fürth sowie die Freie Hansestadt Bremen. Der Förderzeitraum von 1999 bis 2002 wurde durch das BMWA um ein weiteres Jahr bis Ende 2003 verlängert. Ziel aller Preisträgerstädte ist es, zwischen der Verwaltung auf der einen Seite und Bürgern sowie ansässigen Wirtschaftsunternehmen und freiberuflich Tätigen auf der anderen Seite rechtsverbindliche Dienstleistungen und Transaktionen über elektronische Kanäle abwickeln zu können. Der generelle Fokus liegt hierbei auf der Vereinfachung der Verwaltungsabläufe und damit der Verbesserung von Serviceleistungen durch die Verwaltung.

7.3.1 Umsetzung von MEDIA@Komm in Esslingen

Ziel des MEDIA@Komm-Projektes in Esslingen ist es, die virtuelle Stadt mit elektronischem Rathaus und virtuellem Marktplatz modellhaft zu erforschen und zu entwickeln. Im Mittelpunkt steht hierbei das Ziel, rechtsverbindliche Transaktionen im Internet unter Einbindung der elektronischen Signatur möglich zu machen. Dabei setzt man auf Synergien: MediaKomm Esslingen ist ein Verbundprojekt und vereinigt Partner aus Kommunen, der Privatwirtschaft und Forschungsinstitutionen.

Technische Lösung der rechtlichen Anforderungen

Basis aller Anwendungen des MEDIA@Komm-Projekts in Esslingen bildet das Modul „AllSign“. „AllSign" steht hierbei für "Alle Signieren Alles“. Es bietet ein intelligentes Formular-Management-System, mit dem Dokumente und Formulare mit elektronischer Signatur unterzeichnet und die Nutzdaten in Fachapplikationen weitergereicht werden können. Die für den jeweiligen Behördengang erforderlichen Daten werden mittels eines Dialog-Managers bei den Bürgern abgefragt. Mit diesem Out-of-the-Box-Produkt können heute bereits 20 Verwaltungsdienste mit Signatur online abgewickelt werden. „AllSign“ ist die Lösung zur elektronischen Signierung aller Dateiformate, z.B. auch von PDF-Dokumenten. Die Anwenderdaten werden mit Hilfe einer benutzerorientierten und anwenderfreundlichen Dialogbox visualisiert eingegeben. Anschließend werden die Daten im digitalen Work-flow weiterverarbeitet, d.h. die Daten werden auf dem Server in ein PDF-Formular und in eine XML-Datei übertragen. Danach erfolgt die elektronische Unterschrift und das signierte File wird über den Server verifiziert. Die elektronische Unterschrift wird anschließend über das Trust Center geprüft. Diese Vorgehensweise erleichtert dem Anwender das Ausfüllen von Formularen und die Benutzung der elektronischen Signatur erheblich. Ein weiterer Vorteil besteht darin, dass der Benutzer das gewohnte Formular visuell auf dem Bildschirm sehen und zur Archivierung auch ausdrucken kann.

Verarbeitung von personenbezogenen Daten innerhalb der AllSign-Umgebung

Einer der hauptsächlichen Nutzen des Lebenslagenmodells beruht in der Vermeidung von Mehrfacheingaben, wenn eine Anzahl von Anliegen vorgebracht werden sollen. Unter diese Mehrfacheingaben fallen z.B. die Nennung der Personendaten und des Wohnortes, die eine Grundlage für viele Anliegen darstellen und zu deren Bearbeitung notwendig sind. Im Projekt MediaKomm Esslingen hat man sich für einen serverbasierten Einsatz für die Entwicklung der eGovernment-Verfahren entschieden, da dieser sich im Sinne eines mehrstufigen eGovernment-Konzeptes leichter und schneller umsetzen lässt, weniger Ressourcen beim Nutzer voraussetzt und eine einfachere Einbindung von Fachverfahren z.B. zum Zweck der Plausibilisierung ermöglicht. Findet allerdings die Eingabe der Daten für die Anliegen im Rahmen einer Lebenslage in einer serverbasierten Umgebung statt, kommt es auf der technischen Plattform zu einer Kummulierung von personenbezogenen Daten für unterschiedliche Adressaten. Diese Daten werden nach Abschluss der Arbeiten wieder nach Anliegen getrennt aufbereitet und an die einzelnen zuständigen Stellen weitergeleitet. Um den Anforderungen des Datenschutzes gerecht zu werden, findet keine Speicherung dieser Daten auf der Serverplattform statt. Stattdessen befinden sich die Daten lediglich im Arbeitsspeicher des Servers und werden nicht auf einem permanenten Speichermedium dauerhaft abgelegt. Es kann daher keine Auswertung dieser Daten erfolgen. Da man-

che Lebenslagen sehr kompliziert sind und Arbeitsunterbrechungen nicht ausgeschlossen werden können, kann der Bürger die Sitzung auf seinem eigenen PC abspeichern und bei Bedarf zum Server hochladen. Die Verbindung zwischen dem PC des Bürgers und dem eGovernment-Server wird durch das SSL-Protokoll gesichert. Ferner ist durch ein Betriebskonzept vorgesehen, dass der eGovernment-Server auf einer Plattform im gesicherten Bereich einer Kommune betrieben wird. Es ist geplant, das AllSign-Konzept um eine Möglichkeit der anonymisierten Datenverarbeitung zu erweitern, die es erlauben würde, den Server bei einem Dienstleister zu betreiben. Der datenschutzrechtliche Mehrwert dieser Lösung liegt darin, dass der Zugriff auf die Daten im Gegensatz zum papierbasierten Formularwesen durch ein technisches System gewährleistet werden kann.

Datenschutzrechtliche Bewertung:

Das Modul AllSign verbindet das Lebenslagenkonzept und die nutzerfreundliche Vermeidung von Mehreingaben gezielt mit Anforderungen des Datenschutzes. Dem Grundsatz der Datensparsamkeit wird durch eine bloß temporäre Speicherung personenbezogener Daten auf dem Arbeitsspeicher des Servers entsprochen. Die geplante Erweiterung von AllSign um die Möglichkeit der anonymisierten Datenverarbeitung betont zusätzlich die zunehmende Berücksichtigung des Grundsatzes der Datenvermeidung.

7.3.2 Umsetzung von MEDIA@Komm in der Region Nünberg/Fürth

Die Curiavant Internet GmbH entwickelt und vertreibt ein System für die rechtsverbindliche Online-Kommunikation zwischen Bürgern, Unternehmen und Verwaltung. Das Unternehmen wurde im Dezember 1999 als 100-prozentige Tochter von dem Städteverbund Nürnberg, Fürth, Erlangen, Schwabach und Bayreuth zur Realisierung des MEDIA@Komm-Preisträgerkonzepts gegründet. Im Mittelpunkt steht auch hier die erleichterte Abwicklung der Verwaltungsdienstleistungen durch Einsatz moderner Informations- und Kommunikationstechnologien. Die Nutzer der Verwaltungsangebote können den Behördengang via Internet abkürzen und zahlreiche Formalitäten zu Hause am PC oder an öffentlich zugänglichen und betreuten Terminals abwickeln. Grundlage für eine rechtskonforme Abwicklung auch im Falle von bestehenden gesetzlichen Formerfordernissen ist entsprechend der Zielsetzung des Gesamtprojekts MEDIA@Komm die elektronische Signatur nach dem Signaturgesetz (SigG). Für alle Anwendungen sieht das System jeweils auch die Bezahlfunktion vor. Nachfolgend ein paar Beispiele:

Kommunikation zwischen Bürgern und Verwaltung

- An- und Ummeldungen im Einwohnermeldeamt,
- Ausstellung von Anwohner-Parkausweisen,
- Abwicklung von Bauanträgen,
- Buchung von Eintrittskarten (z.B. Oper, Theater) und VHS-Kursen.

Kommunikation zwischen Unternehmen und Verwaltung

- Gewerbeanmeldung,
- Auskünfte aus dem Melderegister,
- Ausschreibung und Vergabe öffentlicher Aufträge,
- Baurechtliche Verfahren.

Über die kommunalen Anwendungen werden folgende Public-Private-Projekte umgesetzt:

- Existenzgründerbetreuung,
- Virtueller Marktplatz,
- ÖPNV Ticketing,
- Betriebsausweise,
- Medizinisches Intranet.

Datenschutz- und Sicherheitsaspekte des MEDIA@Komm-Projektes der Region Nürnberg

Die für die Kommunikation von Kommunen mit Bürgern, Firmen und Verwaltungen zur Verfügung gestellten Geschäftsprozesse, die überwiegend über das Internet abgewickelt werden, erfordern besondere Vorkehrungen in Bezug auf Datenschutz und Datensicherheit. Im MEDIA@Komm-Projekt der Region Nürnberg werden dafür skalierbare Verfahren eingesetzt, die auf elektronischen Signaturen und symmetrischen Verschlüsselungsverfahren basieren. Die elektronische Signatur wird dabei in zwei Funktionen eingesetzt:

- als rechtsverbindliche Unterschrift unter Formularen, Anträgen und Verträgen,

- als Instrument zur rechtsverbindlichen Authentifizierung von Personen, denen danach Rollen und Berechtigungen zugewiesen werden können.

Zur Verschlüsselung werden die sichersten heute bekannten Verfahren mit Schlüssellängen von mindestens 128 bit eingesetzt. Dabei wird zwischen einer Transportverschlüsselung und einer Archivverschlüsselung unterschieden. Beide Verfahren sind so ausgelegt, dass sie einfach und über entsprechende Parameter der jeweiligen Anforderung angepasst werden können. So kann z.B. für den Transport eine einseitige SSL-Verschlüsselung, aber auch eine dezidierte Ende-zu-Ende-Verschlüsselung eingesetzt werden. Auch die Archivverschlüsselung kann in verschiedenen Stufen realisiert werden. Die oben genannten kryptographischen Funktionen werden von der innerhalb des MEDIA@Komm-Projektes entwickelten SignatureEngine bereitgestellt. Die SignatureEngine mit den Funktionen Signieren, Verifizieren, Authentisieren und Verschlüsseln stellt einen der zentralen Bestandteile der kommunalen E-Government Plattform des Städteverbundes dar. Die zentrale Bündelung der Sicherheitsfunktionen ist ein wichtiger Baustein des Sicherheitskonzeptes der Gesamtlösung.
Die beschriebenen Lösungen und die bei der Umsetzung gewonnenen Erfahrungen werden in die Weiterentwicklung des von allen MEDIA@Komm-Städten unterstützten OSCI-Standards eingebracht.

Datenschutzrechtliche Bewertung:

Im Städteverbund Nürnberg werden Signatur- und Verschlüsselungstechniken zur Sicherung datenschutzrechtlicher Aspekte eingesetzt. Durch eine zentrale Bündelung der Sicherheitsfunktionen wird ein gleichbleibend hoher Sicherheitsstandard gewahrt.

7.3.3 Umsetzung von MEDIA@Komm im Bundesland Bremen

Zur Umsetzung des MEDIA@Komm-Projektes Bremen wurde im Herbst 1999 eigens die bremen-online-services GmbH & Co. KG gegründet. Der Bremer-Online-Service stellt dem Bürger, aber auch Architekten, Rechtsanwälten und anderen so genannten „Mittlern“, Dienstleistungen sowohl der öffentlichen Verwaltung als auch privater Dienstleiter zur Verfügung. Die Dienstleistungen werden über das Internet über die Adresse www.bremer-online-service.de offeriert. Die Rechtssicherheit wird, soweit erforderlich, durch eine signaturgesetzkonforme elektronische Signatur gewährleistet.
Als Übertragungsprotokoll für die Kommunikation zwischen Verwaltung und Bürger wird OSCI (Online Service Computer Interface) benutzt. Die Geschäftsprozesse öffentlicher und privater Dienstleister wurden im Bremer Konzept nicht nach Behördenzuständigkeiten, sondern nach Lebenslagen zusammengefasst (z.B. Umzug, Studium, Bau eines Hauses, Freizeit usw.).
Informationstechnisch werden die Dienstleistungen über eine zentrale Plattform realisiert, die von der bremen online services GmbH & Co. KG (bos) als sogenannter Intermediär betrieben wird (siehe Refenrenzandwendung „Governikus“)

Hauptsächliche Funktionen der OSCI-Plattform

- Bereitstellung von Formularen auf einem Formularserver;
- Zielgerichtete Weiterleitung der verschlüsselten und in der Regel gemäß Signaturgesetz (SigG) signierten Formularinhalte in Form von OSCI-Nachrichten an den Empfänger;
- Authentisierung der OSCI-Nachricht anhand des Absenderzertifikats;
- Generierung eines sogenannten Laufzettels, auf dem Auftragsinformationen protokolliert werden;
- Zahlungsabwicklung von Dienstleitungen (bos vergibt im Auftrag der Landeshauptkasse Bremen Kassenzeichen und schickt diese per OSCI an den Bürger);
- Einfügung von Bezahlinformationen in den Laufzettel der OSCI-Nachricht.

Realisierte Anwendungen im bremer-online-service

- Mahnverfahren

Zum 1. Oktober 2001 wurde in Bremen das bereits in zahlreichen Bundesländern praktizierte automatisierte gerichtliche Mahnverfahren eingeführt. Mit ProfiMahn ist z.B. den Rechtsanwälten die Möglichkeit gegeben, mit einer Mahnsoftware erstellte Mahndatensätze per Internet an das Amtsgericht Bremen zu schicken und Mitteilungen des Amtsgerichts aus einem für den Benutzer eingerichteten elektronischen Postfach abzuholen.

- Bauamt

Beim Bau oder Umbau eines Hauses müssen zahlreiche Anträge an das zuständige Bauamt gestellt werden. Über die Plattform des bremen-online-service lassen sich die erforderlichen Formulare und Anträge direkt am PC oder nach dem Ausdrucken ausfüllen. Verschiedene Anträge lassen sich sofort nach dem Ausfüllen über das Internet an das zuständige Amt verschicken. Dort wo der direkte Weg über das Internet noch nicht realisiert ist, wird das Formular per Post dem zuständigen Amt zugestellt. Zu-

sätzlich werden Informationen zum Thema Bauen, wie Gesetzestexte oder Förderprogramme über Links im Angebot des bremen-online-service den Bürgern zur Verfügung gestellt.

- Standesamt

Das Standesamt Bremen bietet über den bremen-online-service den Bürgern die Möglichkeit, diverse Ausfertigungen und Urkunden online anzufordern (z.B. Heiratsurkunde, Geburtsurkunde, Abschriften aus dem Familienbuch); geschieht dies mit einer Signaturkarte (qualifizierte Signatur) werden die Dokumente an die angegebene Adresse versandt, ansonsten müssen die Dokumente persönlich beim Standesamt abgeholt werden. Integriert in das Angebot des Standesamtes ist eine Online-Bezahlmöglichkeit.

- Stadtwerke

Die Stadtwerke Bremen (swb Enordia) haben über den bremen-online-service unterschiedliche Dienstleistungen realisiert und stellen diese den Bürgerinnen und Bürgern online zur Verfügung. Folgende Dienstleistungen sind zum jetzigen Zeitpunkt realisiert:

- Ab- / Anmeldung bei Wohnungseinzug bzw. –auszug,
- Mitteilung des Zählerstandes für die Jahresabrechnung,
- Mitteilung der Bankverbindung,
- Erteilung einer Einzugsermächtigung.

Technische Lösungen der rechtlichen Anforderungen

Aus den rechtlichen Rahmenbedingungen erwachsen für die dargestellten Anwendungen verschiedenste Anforderungen an ihre technische Lösung. Das Modul Governikus wird allen Anforderungen mit eigens für das eGovernment entwickelten Bausteinen, wie z.B. Signatur, Transport und Sicherheit, gerecht. Der Aufbau der Software orientiert sich streng an dem OSCI-Kommunikationsmodell und zentralisiert z.B. die aufwändige Prüfung des Signaturzertifikats des Bürgers. Daneben ermöglicht Governikus eine Abwicklung der genannten Anwendungen auch unter Beachtung datenschutzspezifischer Anforderungen. Durch eine Drei-Schichten-Architektur praktiziert es vor allem die strikte Trennung von „Nutzungs- und Inhaltsdaten“ (Prinzip des „doppelten Umschlags“) für den Vorgang der Datenübermittlung. Diese Trennung schützt die sensiblen und datenschutzrechlich besonders relevanten Inhaltsdaten vor einem unbefugten Zugriff während der Datenübertragung, welche typischerweise in „Offenen Netzen“ stattfindet. Durch die konsequente Trennung von Nutzungs- und Inhaltsdaten ist es bei Verwendung des Governikus-Moduls insbesondere auch möglich, eGovernment-Dienste über Intermediäre (z.B. zentrale Kommunikations- oder Post-Stellen) zu betreiben und gleichwohl datenschutzrechtlichen Grundsätzen wie z.B. der informationellen Gewaltenteilung, Datensparsamkeit und Datenabschottung bestmöglich zu entsprechen. Denn Zugang zu den Inhaltsdaten erhält nur der Adressat des Dokuments. Die Möglichkeit einer darüber hinausgehenden Kenntnisnahme von Inhaltsdaten in den zu durchlaufenden Transportebenen wird vermieden. Der Intermediär überprüft die Signatur des Dokuments und übernimmt die Verteilung in das Back-Office, hierfür besteht für ihn jedoch nur eine Zugriffsmöglichkeiten auf relevante Transportdaten („äußerer Umschlag“ des Dokuments).

Datenschutzrechtliche Bewertung:

Die Governikus-Software gewährleistet die Rechtsverbindlichkeit eines Dokuments sowie die Beachtung von Datenschutz und Datensicherheit. Insbesondere durch das „Prinzip des doppelten Umschlags“ werden sensible Daten vor unbefugter Kenntnisnahme geschützt und hierdurch den datenschutzrechtlichen Anforderungen entsprochen. Gerade an der im eGovernment besonders relevanten Schnittstelle zwischen Intermediären und Back-Office wird den gesetzlichen Datenschutzanforderungen der informationeller Gewaltenteilung, Datensparsamkeit und Datenabschottung gezielt Rechnung getragen.

8 Wichtige Linkadressen

In der Handreichung sind zu den wesentlichen Aussagen und Empfehlungen Internet-Adressen zur weiteren Recherche aufgenommen worden. An dieser Stelle finden Sie noch einmal die wichtigsten übergreifenden Internet-Adressen zum Thema „Datenschutzgerechtes eGovernment“.

Linkadressen	**Stelle - Inhalt**
www.datenschutz.de	Virtuelles Datenschutzbüro
www.modernerStaat.de	Programm der Bundesregierung
www.bundonline2005.de	Internetfähigen Dienstleistungen der Bundesverwaltung bis zum Jahr 2005
www.bsi.de	Bundesamt für Sicherheit der Informationstechnik
www.koop-adv.de	Im Kooperationsausschuss ADV (KoopA ADV), dem der Bund, die Länder und die kommunalen Spitzenverbände angehören, werden die gemeinsamen Grundsätze des Einsatzes der Informations- und Kommunikationstechniken (IT) und wichtige IT-Vorhaben in der öffentlichen Verwaltung besprochen.
www.mediakomm.net	Hier werden Zwischenergebnisse aus den Preisträgerstädten sowie Hintergrundinformationen vorgestellt (Elektronisches Rathaus, Elektronischer Marktplatz, Digitale Signatur usw). Das Forum ermöglicht Ihnen den Informations- und Erfahrungsaustausch. Dieses Portal entwickelt sich dynamisch – wie die MEDIA@Komm Projekte. Angebote und Inhalte werden ununterbrochen erweitert und aktualisiert.

Stichwortverzeichnis