Abgeordnetenhaus von Berlin

Drucksache 9/ 885
29. 12. 82

9. Wahlperiode

28 Seiten

Mitteilungen des Präsidenten

- Nr. 92 -

Inhaltsübersicht | Nr. | Seite

Druckschluß: 22. November 1982, 12.00 Uhr

Ausgegeben am 29. Dezember 1982

Der Präsident
Peter Rebsch

Die Veröffentlichungen des Abgeordnetenhauses sind beim Kulturbuchverlag Berlin, Passauer Straße 4, 1000 Berlin 30, Telefon 2 13 60 71, zu beziehen.

BERICHT
DES BERLINER DATENSCHUTZBEAUFTRAGTEN
zum 31. Dezember 1982

Inhaltsverzeichnis

[1] Nach § 26 Abs. 2 Berliner Datenschutzgesetz berichtet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich.
Es liegen folgende Berichte vor:
- Bericht über die Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten vom Januar 1980, Mitteilungen des Präsidenten – Nr. 40 –, Drucksache 8/277 vom 22. Januar 1980.
- Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1980 (Jahresbericht 1980), Mitteilungen des Präsidenten – Nr. 107 –, Drucksache 8/666 vom 28. Januar 1981.
- Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1981 (Jahresbericht 1981), Mitteilungen des Präsidenten – Nr. 20 –, Drucksache 9/248 vom 29. Dezember 1981.

1. Überblick

1.1 Zur Situation

Das Interesse am Datenschutz ist bei den Berlinern erneut deutlich gewachsen. Dies zeigt die gegenüber dem Vorjahr wiederum erheblich - um ca. 50 % - gestiegene Zahl der Eingaben. Die Bürger können so erreichen, daß der Umgang mit ihren Daten durch die Verwaltung überprüft wird. Die Kontrolle hat zur Folge, daß sich das Verhalten der Verwaltung häufig ändert. Vielfach haben die Eingaben eine über den Einzelfall hinausgehende Bedeutung, wenn sie Schwachstellen der Gesetzgebung oder der Verwaltungspraxis offenbaren.

Die Aktivitäten des Datenschutzbeauftragten erschöpfen sich jedoch nicht in der Reaktion auf Eingaben. Vielmehr gehört es auch zu seinen Aufgaben, bereits den Anfängen von Freiheitsbedrohungen durch Datenverarbeitung - nicht zuletzt beim Aufbau großer automatischer Dateien und beim Herstellen von Verknüpfungen zwischen verschiedenen Dateien - zu wehren und durch frühzeitige Beratung den vielfältigen Gefahren der Verarbeitung personenbezogener Daten vorzubeugen. Diese Tätigkeit mag weniger spektakulär sein als die Aufdeckung eines „Skandals", sie ist aber für den Bürger nicht minder bedeutsam.

Aus diesem Grunde habe ich im folgenden auch auf die Datenschutzbelange bei in der Entwicklung befindlichen ADV-Verfahren und bei sich erst abzeichnenden Regelungen, z. B. auf dem Gebiet der Neuen Medien, des Einwohnermeldewesens und der Sozialgesetzgebung (Sozialgesetzbuch) hingewiesen. Die Vorschläge akzentuieren und ergänzen die bislang bekannten Entwürfe und weisen den Parlamentariern Alternativen für ihre Entscheidungen auf.

1.2 Fortentwicklung der Datenschutzvorschriften

Bereits in meinem Jahresbericht 1980[2] hatte ich darauf hingewiesen, daß angesichts der Subsidiarität der Datenschutzgesetze zunehmend spezialgesetzliche Regelungen geschaffen werden.

Dem damit verbundenen Bestreben, den Datenschutz bereichsspezifisch zu verbessern, steht die ebenfalls zu beobachtende Tendenz gegenüber, bestehende datenschutzrechtliche Barrieren durch Spezialgesetze aus dem Wege zu räumen und den Zugang zu Datenbeständen verschiedenster Art zu eröffnen.

Wichtige Beispiele für diese Tendenz bieten die Gesetze, die Ende 1981 zur Absicherung des Haushaltes 1982 erlassen worden sind. In sogenannten „Artikelgesetzen", insbesondere dem Gesetz zur Bekämpfung der illegalen Beschäftigung[3] und dem Zweiten Haushaltsstrukturgesetz[4], wurde eine Vielzahl einzelner Vorschriften aus den verschiedensten Gesetzgebungsbereichen mit dem Ziel geändert oder neu geschaffen, Ausgaben zu vermindern oder zusätzliche Einnahmen zu schaffen; in vielen Fällen wurden zu diesem Zweck neue Informationsverpflichtungen begründet.

Das *Gesetz zur Bekämpfung der illegalen Beschäftigung* verpflichtet so die Bundesanstalt für Arbeit, die Krankenkassen, die Träger der Unfallversicherung, die zur Bekämpfung der Schwarzarbeit eingerichteten Behörden, die Ausländerbehörden und die für den Arbeitsschutz zuständigen Behörden zur gegenseitigen Unterrichtung nicht nur über Verstöße gegen sozial- und arbeitsrechtliche Bestimmungen, sondern auch über Verstöße gegen das Ausländergesetz und gegen Steuergesetze. Unter Aufhebung des Steuergeheimnisses werden ferner die Finanzbehörden zur Übermittlung entsprechender Daten an die Bundesanstalt für Arbeit ermächtigt. Die Konsequenz derartiger Verpflichtungen ist nicht nur die Einrichtung einer Vielzahl entsprechender Informationsflüsse, sondern auch das Entstehen von Datensammlungen, für die in den Gesetzen keinerlei spezielle Tilgungsvorschriften enthalten sind.

Ohne erkennbaren Zusammenhang mit dem Gesetzeszweck enthält das Gesetz zur Bekämpfung der illegalen Beschäftigung zwei Bestimmungen, die über den Bereich der Bekämpfung der Schwarzarbeit hinaus Bedeutung haben und zu erheblichen datenschutzrechtlichen Problemen geführt haben:

In Art. 2 des Gesetzes wird § 205 Abs. 4 Satz 2 *Reichsversicherungsordnung* dahingehend geändert, daß bei der Gewährung von Familienkrankenhilfe (z. B. von Leistungen für die ärztliche Behandlung von Kindern), für die mehrere Krankenkassen in Betracht kommen, nunmehr die Krankenkasse desjenigen Versicherten leisten muß, für den im letzten Monat vor Eintritt des Leistungsfalles der höhere Beitrag zu entrichten war. Dies führte zu folgender Konsequenz: Während bei getrennt lebenden oder geschiedenen Eltern früher diejenige Krankenkasse Krankenscheine für Kinder ausstellte, bei der zuerst der Antrag gestellt wurde (in der Regel die Krankenkasse der Mutter), ist nunmehr vor der Ausstellung der Krankenscheine zu überprüfen, welcher Elternteil einen Monat vor Eintritt des Leistungsfalles höhere Beiträge gezahlt hat. Da häufig getrennt lebende Eltern nicht wissen, wo der jeweilige andere Elternteil krankenversichert ist, geschweige denn, welche Beiträge er zur Krankenversicherung zahlt, verpflichtet die neue Regelung zur Offenbarung von Informationen, die gar nicht zu beschaffen sind.

Dies ging in einem mir vorgetragenen Fall so weit, daß einer Mutter, die von ihrem Recht Gebrauch gemacht hatte, den Namen des Kindesvaters nicht zu benennen, die Ausstellung von Krankenscheinen für das Kind verweigert wurde. In diesem Fall hat die zuständige Kasse auf die Offenbarung verzichtet.

In anderen Fällen konnte dadurch Abhilfe geschaffen werden, daß die Krankenkasse eigene Nachforschungen anstellte. Dies ändert jedoch nichts an der Tatsache, daß der Gesetzgeber eine wegen der damit verbundenen Informationspflichten kaum vollziehbare Vorschrift geschaffen hatte.

Weniger plakativ, dafür aber in den Konsequenzen erheblich weitgehender dürfte die in Artikel 7 vorgenommene Änderung des erst seit 1. Januar 1981 geltenden *Sozialgesetzbuches X* (SGB X) sein: Während Sozialdaten an Finanzbehörden bis dahin nur offenbart werden durften, wenn zuvor ein Auskunftsersuchen bei den Beteiligten gescheitert war oder der Verdacht einer Steuerstraftat vorlag, wurden in § 71 Nr. 3 SGB X nunmehr unabhängig vom Zweck der Bekämpfung der Schwarzarbeit die allgemeinen Amtshilfevorschriften für anwendbar erklärt und damit der Schutz der Sozialdaten vor der unbeschränkten Offenbarung gegenüber den Finanzbehörden aufgehoben. Eine Resolution der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in der eine Begrenzung auf die Zwecke der Bekämpfung der Schwarzarbeit gefordert worden war, hat der Gesetzgeber nicht berücksichtigt.

Unter der Vielzahl der im *Zweiten Haushaltsstrukturgesetz* enthaltenen Regelungen mit datenschutzrechtlichen Konsequenzen seien hervorgehoben:

Änderungen des *Beamtenversorgungsgesetzes* hatten Auswirkungen auf die Anrechnung weiterer Versorgungsbezüge. Die Folge ist die Notwendigkeit der zusätzlichen Erhebung von Daten über sämtliche Einkünfte von Versorgungsempfängern, insbesondere auch von Grund und Herkunft zusätzlicher Versorgungsleistungen. Die damit verbundene Verpflichtung zum Ausfüllen ausführlicher Fragebogen wurde von vielen Versorgungsempfängern als Beeinträchtigung empfunden.

Die im *Bundessozialhilfegesetz* verstärkte Berücksichtigung des Einkommens der Unterhaltsverpflichteten bei Behinderten führte dazu, daß dieser Personenkreis nunmehr weitgehende Auskunftsverpflichtungen über Einkommens- und Vermögensverhältnisse unterliegt und verpflichtet ist, in die Offenbarung personenbezogener Daten durch dritte Stellen, insbesondere Banken einzuwilligen. Diese Regelung ist auch in der überregionalen Presse auf heftige Kritik gestoßen.

Im Rahmen des Zweiten Haushaltsstrukturgesetzes wurden verschiedene wohnungsrechtliche Bestimmungen geschaffen oder geändert mit dem Ziel, Fehlsubventionierung und Mietverzerrung im Wohnungswesen abzubauen. Das in Unterartikel 1 verkündete *Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen* verpflichtet einerseits die Mieter von Sozialwohnungen zur Offenbarung ihrer Einkommensverhältnisse nicht nur gegenüber der nach dem Gesetz zu schaffenden Behörde, sondern auch zur Offenbarung untereinander (z. B. der Untermieter gegenüber dem Hauptmieter). Soweit das Gesetz es erfordert,

[2] S. 3

[3] Bundesgesetzblatt I, S. 1390 ff. vom 19. Dezember 1981

[4] Bundesgesetzblatt I, S. 1523 ff. vom 22. Dezember 1981

werden alle Behörden zur Auskunftserteilung über Einkommensverhältnisse verpflichtet, wiederum unter Beschränkung des Steuergeheimnisses auch die Finanzbehörden. Zu den Schwierigkeiten, die mit dem Vollzug der Vorschrift insbesondere im Hinblick auf die erforderlichen Datensammlungen verbunden waren, habe ich im folgenden unter 2.1 Stellung genommen.

Zu bedenklichen Konsequenzen hat schließlich auch das 9. *Gesetz zur Änderung des Bundeskindergeldgesetzes* geführt: Die veränderten Bestimmungen über die Einbeziehung des Einkommens von Ehegatten derjenigen Kinder, für die Kindergeld bezogen wird, führten u. a. zu dem Ansinnen, daß Auskünfte über die Einkommensverhältnisse der Ehegatten von Kindern zu machen waren. Hier ist ähnlich wie bei der Neufassung des § 205 Abs. 4 Satz 2 Reichsversicherungsordnung ein verfassungsrechtlich bedenklicher Eingriff in die Persönlichkeitsrechte der Betroffenen festzustellen. Auf die Geltendmachung meiner Bedenken hin hat der Berliner Senator für Inneres auf die Erhebung dieser Daten beim Antragsteller verzichtet und die Behörden auf die Einholung der Auskünfte bei den Betroffenen verwiesen.

Diese Beispiele zeigen, daß bei Gesetzesänderungen die praktischen Auswirkungen auf Datenerhebung und Datenverarbeitung nicht immer entsprechend berücksichtigt werden. Bei bestimmten Fallkonstellationen ist das Haushaltsstrukturgesetz nicht zu vollziehen. Im übrigen ist zu bedenken, daß man im Glauben, man könne durch neue Informationsflüsse und -sammlungen Kosten senken, zu allererst - z. T. erhebliche - Kosten verursachende Maßnahmen veranlaßt.

Neben der Frage, ob der mit der beabsichtigten Einsparung verbundene erhöhte Verwaltungsaufwand verhältnismäßig ist, stellt sich die Frage, ob nicht auch bei Einsparungsvorschriften Persönlichkeitsrechte entsprechend gewahrt werden können.

Die in der Regel für den Vollzug verantwortlichen Landesbehörden sollten im Rahmen ihrer Einwirkungsmöglichkeiten auf das Gesetzgebungsverfahren auch des Bundes verstärkt auf die datenschutzrechtlichen Aspekte derartiger Gesetzgebungsvorhaben achten. Das stärkere Engagement der Bürger in Datenschutzfragen ist somit auch eine gute Chance, bei der Gesetzgebung nicht gesehene und ggf. nicht gewollte praktische Auswirkungen zu korrigieren und bei neuen Gesetzen diesen Gesichtspunkt stärker als bisher zu beachten.

2. Kontrolle der Einhaltung der Datenschutzvorschriften

- Schwerpunkte -

Die für 1982 vorgesehenen Schwerpunkte[5] - Überprüfungen im Bereich Bau- und Wohnungswesen, Neue Medien, öffentliche Sicherheit und Strafverfolgung sowie Überprüfungen von Rechenzentren und Rechenstellen - konnte ich, wie vorgesehen, in Angriff nehmen.

2.1 Bau- und Planungswesen

Die Überprüfungen im Bereich des Bau- und Planungswesens haben durch zahlreiche Eingaben und parlamentarische Anfragen[6] zusätzliche Aktualität erhalten. Nicht zuletzt auf der Ebene der Bezirke sind Datenschutzprobleme in Zusammenhang mit Baufragen z. T. heftig diskutiert worden.

Ein großer Teil der vielfältigen Fragen läßt sich im wesentlichen auf die Frage zurückführen, welche Publizität personenbezogene Daten bei Bauvorgängen (von der Baugenehmigung oder der Umwandlung von Mietwohnungen in Eigentumswohnungen bis hin zur Abrißgenehmigung) haben sollen.

Über meine Stellungnahme zu den Einzelfällen hinausgehend habe ich dem Senator für Bau- und Wohnungswesen empfohlen, den Bezirksämtern eine einheitliche Leitlinie, etwa in Gestalt eines Rundschreibens, an die Hand zu geben, um der zum Teil erheblichen Verunsicherung zu begegnen und eine einheitliche Praxis zu gewährleisten.

[5] Vgl. Jahresbericht 1981, 6.1, S. 18/19

[6] Z. B. Kleine Anfrage Nr. 949 v. 29. April 1982 (vgl. Drucksache 9/669, S. 9) Kleine Anfrage Nr. 1137 v. 22. Juli 1982 (vgl. Drucksache 9/688, S. 2)

Versendung von Mieterlisten

Zahlreiche Mieter haben sich an mich gewandt und geltend gemacht, durch die Praxis der Versendung von Mieterlisten durch die Mietpreisstellen der Bezirksämter in ihren Rechten verletzt zu werden. Die Mietpreisstellen hatten im Rahmen von Mieterhöhungsverfahren den vollständigen Ausdruck aller Mieterdaten versandt und dabei in mehreren Fällen bis zu 300 personenbezogene Datensätze über Mieter und deren Angehörige an jeden Mieter übermittelt. In einem Bezirksamt hat das Problem zu einer Anfrage in der Bezirksverordnetenversammlung geführt; ferner wurde die Frage im Unterausschuß „Berliner Datenschutzgesetz" des Abgeordnetenhauses aufgegriffen.

Da die Daten aus Dateien übermittelt werden, ist die Weitergabe der Mieterlisten ohne Einwilligung der Mieter nur zulässig, wenn eine Spezialnorm § 11 Berliner Datenschutzgesetz verdrängt.

Der Senator für Bau- und Wohnungswesen sieht in der Beteiligtenregelung der §§ 13, 28 Verwaltungsverfahrensgesetz eine solche Norm. Dem habe ich widersprochen: Da sich die Genehmigung nicht unmittelbar auf die Miethöhe auswirkt, braucht die Behörde die zur Wahrnehmung der Beteiligtenrechte erforderlichen Daten erst nach einem entsprechenden Antrag zu offenbaren (§ 13 Abs. 2 Verwaltungsverfahrensgesetz). Dessen ungeachtet wäre der Umfang der übermittelten Daten auch im Rahmen der Beteiligungsstellung unverhältnismäßig.

Ich habe daher das Verfahren beanstandet und empfohlen, die Mieterlisten erst dann zur Verfügung zu stellen, wenn die Betroffenen die Beteiligtenstellung erlangt haben.

Mitteilung über die bevorstehende Umwandlung von Miet- in Eigentumswohnungen

Einzelne Bezirksämter verschickten an die Mieter eines Hauses, für welches der Eigentümer beim Bau- und Wohnungsaufsichtsamt eine Abgeschlossenheitsbescheinigung im Sinne des Wohnungseigentumsgesetzes beantragt hatte, eine Information über die möglicherweise bevorstehende Umwandlung der Mietwohnungen in Eigentumswohnungen.

Zwar wurden mit dem dabei verwendeten Informationsschreiben an die Mieter keine weiteren personenbezogenen Daten des Eigentümers weitergegeben. Auch bei Informationen über wirtschaftliche Planungen handelt es sich jedoch um Angaben über sachliche Verhältnisse der Eigentümer und damit um personenbezogene Daten, wenn der Eigentümer eine natürliche Person (und nicht z. B. eine Kapitalgesellschaft) ist.

§ 11 Berliner Datenschutzgesetz wird hier in der Regel nicht anwendbar sein, da die Daten nicht aus einer Datei übermittelt werden. Da eine spezielle Offenbarungsvorschrift im vorliegenden Fall fehlt, wird der in § 11 Berliner Datenschutzgesetz festgelegte Rechtsgedanke aber bei der Auslegung von § 30 Verwaltungsverfahrensgesetz zu berücksichtigen sein. Dort ist festgelegt, daß persönliche Geheimnisse oder Betriebsgeheimnisse (mithin werden hier auch Daten juristischer Personen mit umfaßt) unbefugt nicht offenbart werden dürfen. Fehlt wie hier eine ausdrückliche Befugnisnorm, hat eine Abwägung stattzufinden, die dem Geheimhaltungsinteresse des Eigentümers an seiner wirtschaftlichen Planung hinreichendes Gewicht zumißt. Dies wird in der Regel bedeuten, daß ohne die Einwilligung des Eigentümers eine entsprechende Mitteilung an die Mieter nicht zulässig ist.

Diese Auffassung wurde von den beteiligten Senatsverwaltungen im wesentlichen anerkannt.

Offenbarung personenbezogener Daten an Bezirksverordnetenversammlungen und deren Gremien

Mehrfach war die Frage zu klären, in welchem Umfang personenbezogene Daten aus dem Bereich des Bau- und Wohnungswesens an Bezirksverordnetenversammlungen oder deren Gremien offenbart werden dürfen. So wurde im Rahmen einer Kleinen Anfrage im Abgeordnetenhaus die Frage aufgeworfen, inwieweit es mit dem Berliner Datenschutzgesetz vereinbar sei, daß seit längerer Zeit in Vorlagen an die Bezirksverordnetenversammlung Listen von Modernisierungs- und Abrißanträgen der Öffentlichkeit bekanntgegeben werden und diese Listen auch die

Namen der Eigentümer, die Räumungsklagen eingereicht haben, enthalten. In einer Großen Anfrage der Fraktion der Alternativen Liste in der Bezirksverordnetenversammlung Neukölln wurde Auskunft über den Umfang eingeräumter Erbbaurechte verlangt und in diesem Zusammenhang die Angabe der Erbbaurechtsnehmer nebst weiterer personenbezogener Angaben zum Erbbaurechtsvertrag, zur Nutzungsart, zum Erbbauzins, zum Verkehrswert, zur Grundstücksfläche etc. verlangt. Der Ausschuß für Bauwesen der Bezirksverordnetenversammlung Charlottenburg bat mich um Beratung zu der Frage, ob es zulässig sei, daß die Abteilung Bauwesen Kleine Anfragen mit dem pauschalen Hinweis auf § 30 Verwaltungsverfahrensgesetz ablehne.

Soweit das Berliner Datenschutzgesetz Anwendung findet, insbesondere wenn die Daten aus einer automatischen Datei übermittelt werden sollen, gibt § 17 einen Anhaltspunkt: Auf Anfrage der Bezirksverordnetenversammlung, ihrer verfassungsmäßigen Organe sowie ihrer Fraktionen können personenbezogene Daten dann herausgegeben werden, wenn sich die Angabe auf Name, Titel, akademische Grade, die Anschrift sowie ein Merkmal (z. B. Erbbauberechtigte) beschränkt. Weitere Merkmale (z. B. über finanzielle und vertragliche Umstände) dürfen nicht enthalten sein.

Bei anderen Datensammlungen, insbesondere bei der Übermittlung einer Vielzahl von Daten aus Akten, kann die Bewertung angesichts des in den Art. 2 und 1 Grundgesetz verankerten Persönlichkeitsrechts nicht anders ausfallen.

Etwas anderes muß allerdings gelten, wenn die Bezirksverordnetenversammlung oder ihre Gremien im Rahmen ihrer in der Berliner Verfassung sowie im Bezirksverwaltungsgesetz festgelegten Aufgaben tätig werden. Soweit dies zur Aufgabenerfüllung erforderlich ist, sind *diesen Gremien* auch personenbezogene Daten zu offenbaren bzw. Akteneinsicht zu gewähren.

Für die Weiterleitung dieser Angaben an die Öffentlichkeit (dies ist in der Regel mit der Beantwortung von Anfragen verbunden) ist allerdings von allen Beteiligten wiederum § 30 Verwaltungsverfahrensgesetz zu beachten. Da eine ausdrückliche Publizitätsvorschrift auch hier in der Regel nicht vorliegt, setzt die Befugnis eine Abwägung voraus, bei der den schutzwürdigen Belangen der Betroffenen Rechnung zu tragen ist. Diese Abwägung wird insbesondere bei Angaben, die einen Einblick in Vermögensverhältnisse gestatten, zur Unzulässigkeit der Offenbarung führen.

Veröffentlichung personenbezogener Daten im Bebauungsplan und Offenbarungsbefugnis aus Bauakten

Auf Grund von Eingaben und einer Kleinen Anfrage im Abgeordnetenhaus habe ich zum bisherigen Verfahren, Namen und Anschrift von Eigentümern im Bebauungsplan zu veröffentlichen, sowie zur Praxis einiger Bauämter, im Rahmen der Stadtsanierung Bauaufträge der Öffentlichkeit bekannt zu geben, wie folgt Stellung genommen:

Die einschlägigen Rechtsvorschriften in §§ 9, 14 Bundesbaugesetz sowie die nach Landesrecht ergangenen Ausführungsvorschriften enthalten mit Ausnahme des Beteiligungsrechtes der Nachbarn im Interesse des Nachbarschutzes keine Befugnis zur Offenbarung von personenbezogenen Eigentümer- bzw. Bauherrendaten. Auch die Grundbuchordnung gestattet in § 12 nur, im Einzelfall und bei Vorliegen eines berechtigten Interesses Einsicht in das Grundbuch zu gewähren. Hinzu kommt, daß der Bebauungsplan eine Rechtsnorm ist, und Rechtsnormen grundsätzlich keine personenbezogenen Daten enthalten dürfen.

Auch eine Datenoffenbarung nach dem Städtebauförderungsgesetz muß sich im Rahmen der dort getroffenen Regelung halten. Die einschlägigen Vorschriften in §§ 2, 4 und 8 Städtebauförderungsgesetz enthalten zwar allgemeine Aufforderungen zur gegenseitigen Mitwirkung, insbesondere der betroffenen Mieter, jedoch keine ausdrückliche Befugnis, personenbezogene Daten aus den der Behörde bekannten Vorgängen zu offenbaren. Es ist zwar nicht auszuschließen, daß im Rahmen der Mitwirkung, Beteiligung und der Zusammenarbeit der Betroffenen, d. h. der Sanierungsträger (Eigentümer, Mieter, Beratungsvereine etc.) personenbezogene Daten gegenseitig ausgetauscht werden. Eine Offenbarungsbefugnis der Behörden ist im Gesetz jedoch nicht enthalten, da die Behörden sich immer nur an den jeweils Betroffenen im Rahmen der Aufgabenerfüllung wenden können und sollen.

Mangels einer gesetzlichen Offenbarungsbefugnis können damit auch bei der Bauplanung nur Daten im Rahmen des § 30 Verwaltungsverfahrensgesetz offenbart werden.

Die Senatsverwaltung für Bau- und Wohnungswesen hat sich der von mir vertretenen Auffassung angeschlossen.

Kontrolle der für Sanierungszwecke erhobenen Daten

Mehrere Bürger hatten sich mit der Vermutung an mich gewandt, im Zusammenhang mit Sanierungsvorhaben erhobene Vermögensdaten der Mieter würden in Einzelfällen von öffentlichen Stellen an Vermieter weitergegeben. Die Vermieter würden diese Daten zur Durchsetzung ihrer Position bei Verhandlungen über Renovierungen oder Umsetzungen in andere Wohnungen verwenden.

Ich habe daraufhin die Erhebung und Aufbewahrung personenbezogener Daten im Zuge der Stadtsanierung systematisch überprüft und sowohl beim Senator für Bau- und Wohnungswesen als auch in den Bezirken vor Ort Kontrollen vorgenommen. Die von den Bürgern geäußerte Vermutung hat sich nicht bestätigt. Allerdings haben meine Feststellungen ergeben, daß die mit dem Sanierungsverfahren und seinen rechtlichen Grundlagen verbundenen Unsicherheiten auch die Behandlung personenbezogener Daten betreffen.

Personenbezogene Daten fallen in drei Phasen der Sanierung an:

- Bei der vorbereitenden Untersuchung,
- beim Sozialplan,
- bei den Betroffenenratswahlen zur Bürgerbeteiligung.

Die Erhebung dieser Daten war in keinem Fall zu beanstanden. Als Problem hat sich vor allem die Frage erwiesen, wie lange die einmal erhobenen Daten aufzubewahren sind. Ich habe festgestellt, daß Tausende von Karteikarten zum Sozialplan und zahlreiche Ordner, die Einzelfragebogen enthalten, in verschiedenen Bezirksämtern vernichtet werden müssen, da sie für die Verwaltungsarbeiten, für die sie erhoben worden sind, nicht mehr erforderlich sind.

Die Erforderlichkeit zur Aufgabenerfüllung nach §§ 4 ff. Städtebauförderungsgesetz läßt sich hinsichtlich der erhobenen Daten nach folgenden Kriterien beurteilen:

- Stand der Sanierung
- Alter der Daten.

Bei Daten aus der vorbereitenden Untersuchung ist die Aufbewahrung generell unzulässig, wenn die wissenschaftliche Auswertung abgeschlossen ist (§ 14 Abs. 3 Berliner Datenschutzgesetz).

Soweit die in den Sozialplankarteien enthaltenen Angaben veraltet sind (durch Fluktuation etc.), sind sie zur Aufgabenerfüllung nicht mehr erforderlich (§ 14 Abs. 3 Berliner Datenschutzgesetz).

Ich habe angesichts der festgestellten Unsicherheiten dem Senator für Bau- und Wohnungswesen und den Mieterberatungsgruppen empfohlen, ein Datenschutzkonzept zu entwickeln. Dieses sollte zumindest folgende Punkte beinhalten:

a) Es ist sicherzustellen, daß der Verbleib der Karteikarten jederzeit nachvollziehbar ist. Möglichst sollten diese an einem Ort stehen und nur einem begrenzten Personenkreis zugänglich sein.

b) Die Löschung von Daten, deren Verwendung in der Zukunft noch nicht gesichert ist, sollte durch die Festlegung von Löschungsfristen, die der „Alterungsfrist" entsprechen, vorbereitet werden. Bis zum Löschungszeitpunkt sind sie sicher aufzubewahren (vgl. Anlage zu § 5 Berliner Datenschutzgesetz).

c) Der Senator für Bau- und Wohnungswesen soll durch geeignete Maßnahmen die Kontrolle der Einhaltung der Datenschutzregelungen im Bereich der Sanierungsverwaltung übernehmen.

In einer weiteren Prüfung werde ich feststellen, ob den Belangen des Datenschutzes in diesen Bereichen nunmehr Rechnung getragen wird.

Fehlbelegungsabgabe

Durch das Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen (AFWoG) wurde die Senatsverwaltung für Bau- und Wohnungswesen vor das Problem gestellt, eine möglichst vollständige Datei über die Bewohner von subventionierten Wohnungen zu erstellen, um auf dieser Grundlage die zu entrichtende Abgabe einzuziehen. Da ich sehr frühzeitig beteiligt worden bin, konnte ich Vorschläge für die Organisation der Datenverarbeitung unterbreiten, die in den vom Senat am 21. April 1982 getroffenen Beschlüssen zum Aufbau einer zentralen Datei beim Landesamt für Wohnungswesen berücksichtigt worden sind.

Beim jetzigen Stand der gesetzlichen Aufgabenbestimmung ist diese Stelle dazu prädestiniert, die Aufgaben nach dem Wohnungsbindungsgesetz wie auch nach dem AFWoG wahrzunehmen. Für den Fall einer späteren dezentralisierten Erfüllung dieser Verwaltungsaufgabe müßte erneut geklärt werden, wie die Belange des Datenschutzes gewahrt werden können.

Zugriffsberechtigung auf das Liegenschaftskataster

Typisch für eine Reihe von Problemen, die sich in der Berliner Verwaltung für den Einsatz der Datenverarbeitung ergeben, ist eine Fragestellung, die sich für das Liegenschaftskataster ergibt:

Die Verwaltungskompetenz liegt - von Ausnahmen abgesehen - bei den Bezirken, das Verfahren wird jedoch zentral entwickelt und zentral auf einem Rechner des Landesamtes für Elektronische Datenverarbeitung durchgeführt. Speichernde Stellen und damit fachlich und datenschutzrechtlich verantwortlich bleiben jedoch nach der fortbestehenden - nicht geänderten - Gesetzeslage die Bezirksämter.

Der Senator für Bau- und Wohnungswesen vertritt die Ansicht, ihm stehe dessenungeachtet der unbeschränkte Zugriff auf das Liegenschaftskataster zu. Dem kann nicht gefolgt werden. Die Benutzung der Dateien der jeweiligen Bezirke durch die Senatsverwaltung für Planungszwecke ist rechtlich nur zulässig, wenn in jedem Einzelfall angefragt wird oder - was sich bei der vorliegenden Konstellation anbietet - eine generelle Vereinbarung über die Vornahme bestimmter Auswertungen vorliegt. Sinnvollerweise sollte eine derartige Vereinbarung bereits mit der Planung eines Projektes verbunden werden, da anderenfalls die praktischen Vorteile der zentralen Durchführung eines ADV-Verfahrens gar nicht ausgeschöpft werden können.

2.2 Neue Medien

Fortentwicklung der Datenschutzregelungen

Neue Informations- und Kommunikationsmöglichkeiten für jedermann, die sich aus der Einrichtung großer Übertragungskapazitäten („Verkabelung") und der Verknüpfung von Nachrichten-, Fernseh- und Datenverarbeitungstechnologie ergeben, traten im vergangenen Jahr stärker als bisher in den Vordergrund des öffentlichen Interesses. Die Diskussion wurde unter dem Begriff „Neue Medien" zusammengefaßt.

Hatte Berlin durch die Erprobung des Bildschirmtextsystems bereits bisher hieran starken Anteil, so werden in naher Zukunft auch die neuartigen Möglichkeiten des Kabelfernsehens im sogenannten „Kabelpilotprojekt Berlin" von einem ausgewählten Teilnehmerkreis getestet werden können. Hieran wird sich die Einführung eines flächenmäßig umfassenderen Kabelfernsehsystems anschließen, das u.a. die von der Post in Berlin als einer der ersten Großstädte zur Verfügung gestellte Glasfasertechnologie nutzen wird.

Bereits im Jahresbericht 1980[7] hatte ich darauf aufmerksam gemacht, daß mit dieser Entwicklung Datenschutzprobleme bedeutenden Ausmaßes verbunden sind: In dem durch die Neuen Medien verbreiteten Programmangebot können personenbezogene Daten übermittelt werden, deren Verbreitung schutzwürdige Belange der Betroffenen beeinträchtigen, die Speicherung von Benutzungsdaten zum Zwecke des Verbindungsaufbaus, der Abrechnung, aber auch der Benutzungsforschung kann zu Kontroll- und Überwachungszwecken benutzt und mißbraucht werden, die geplante Einrichtung von Fernmeß- und Fernwirksystemen kann mit einem bisher ungeahnten Eindringen außenstehender Stellen in die Privatsphäre verbunden sein.

In Zusammenhang mit der Verabschiedung des Berliner Bildschirmtexterprobungsgesetzes hatte ich eine Reihe von Thesen zur Gewährleistung des Datenschutzes vorgebracht. Im Dezember 1980 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Grundsätze für den Datenschutz bei den Neuen Medien" beschlossen.

Im Anschluß hieran führte ich die Überlegungen fort und faßte das Ergebnis unter dem Titel „Vorstellungen über datenschutzrechtliche Anforderungen an Gesetze auf dem Gebiet der Neuen Medien" zusammen. Sie sind im Anhang 1 diesem Bericht beigefügt. Zentraler Bezugspunkt der Vorschläge ist die Forderung, daß die Länder die Initiative zur Regelung der neuen Materie einschließlich der Datenschutzaspekte ergreifen und den Betrieb der einzelnen Systeme unter ihrer Aufsicht behalten.

Am 4. März 1982 beschlossen die Ministerpräsidenten der Länder, zunächst für das Bildschirmtextsystem eine derartige Initiative zu ergreifen und einen Staatsvertrag über Bildschirmtext zu erarbeiten, auf dessen Grundlage das System nach Abschluß der Erprobungsphase endgültig in Betrieb genommen werden kann. Zwar stehen die Ergebnisse der sowohl in Nordrhein-Westfalen als auch in Berlin durchgeführten Begleituntersuchungen zu den Datenschutzaspekten noch aus. Unter dem Vorbehalt der dort noch zu erwartenden Ergebnisse haben sich die Datenschutzbeauftragten des Bundes und der Länder dennoch bereitgefunden, an der Entwicklung von spezialrechtlichen Datenschutzbestimmungen für diesen Staatsvertrag mitzuwirken. Sie schlugen folgende Formulierung vor:

1. Artikel 9 erhält folgende Fassung:

Artikel 9

(1) Soweit in diesem Staatsvertrag nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden.

(2) Wer zur Nutzung von Bildschirmtext technische Einrichtungen für andere bereitstellt (Betreiber), darf personenbezogene Daten über die Inanspruchnahme einzelner Angebote nur erheben und speichern, soweit und solange diese erforderlich sind, um

1. den Abruf von Angeboten zu vermitteln (Verbindungsdaten),
2. die Abrechnung der für die Inanspruchnahme der technischen Einrichtungen und der Angebote seitens des Teilnehmers zu erbringenden Leistungen zu ermöglichen (Abrechnungsdaten).

(3) Abrechnungsdaten nach Abs. 2 Nr. 2 sind so zu speichern, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter, von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Teilnehmer beantragt eine andere Art und Weise der Speicherung.

(3a) Die Übermittlung von Abrechnungs- und Verbindungsdaten an Dritte ist unzulässig.

(3b) Die Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Verbindungsdaten nach Absatz 2 Nr. 1 sind nach Ende der jeweiligen Verbindung zu löschen.

(4) Absätze 2, 3, 3a und 3b gelten entsprechend für Einzelmitteilungen.

(5) Für das Bereithalten personenbezogener Daten als Inhalt von Angeboten sind ohne Rücksicht darauf, ob die Daten in einer Datei verarbeitet werden, die für den Anbieter geltenden Vorschriften über den Datenschutz anzuwenden.

[7] S. 11

(6) Der Anbieter darf vom Teilnehmer personenbezogene Daten nur erheben und diese verarbeiten, wenn das Erbringen der Leistung oder die Abwicklung des Vertragsverhältnisses anderenfalls unmöglich wäre. Werden Daten des Teilnehmers vom Anbieter gespeichert oder übermittelt, ist der Teilnehmer hierauf vor der Erhebung besonders hinzuweisen. Diese Daten dürfen ohne Einwilligung des Betroffenen nur im Rahmen der Zweckbestimmung der vereinbarten Leistung verarbeitet werden. Das Erbringen der Leistung darf nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung seiner Daten außerhalb der in Satz 3 genannten Zweckbestimmung einwilligt. Die Einwilligung kann auch über Bildschirmtext abgegeben werden.

(7) Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsansprüche nach Datenschutzrecht richten sich gegen den Anbieter, soweit personenbezogene Daten den Inhalt von Angeboten betreffen, im übrigen gegen den Betreiber.

(8) Betreiber und Anbieter haben die technischen und organisatorischen Maßnahmen zu treffen, die über die Vorschriften des Datenschutzgesetzes hinaus erforderlich sind, um sicherzustellen, daß

- die Verbindungsdaten unmittelbar nach Ende der Verbindung gem. Absatz 3 b Satz 2 gelöscht werden,
- der Teilnehmer personenbezogene Daten nur durch eine eindeutige und bewußte Handlung übermitteln kann und
- die zu Zwecken der Datensicherung vergebenen Codes einen dem Stand der Technik entsprechenden Schutz vor unbefugter Kenntnisnahme und Verwendung bieten.

(9) Die jeweils zuständigen Landesbeauftragten für den Datenschutz überwachen die Einhaltung der Vorschriften über den Datenschutz bei dem Betreiber. Die Kontrollbefugnisse sonstiger Stellen bleiben unberührt.

2. Nach Artikel 9 wird folgender Artikel 9a eingefügt:

Artikel 9a
Geheimhaltung

Die bei den Bereitstellungseinrichtungen tätigen Personen sind zur Geheimhaltung der bei ihrer Tätigkeit bekanntgewordenen Tatsachen verpflichtet.

3. In Artikel 10 wird folgender Satz angefügt:

„Das Erheben personenbezogener Daten bei sonstigen Meinungsumfragen ist verboten."

Im Interesse der Rechtsklarheit würden die Datenschutzbeauftragten eine eindeutige Regelung über die Trägerschaft der Bildschirmtextzentrale begrüßen, da die Anwendung der in Artikel 9 Abs. 1 genannten Datenschutzbestimmungen davon abhängt.

Ausnahmen für die Bundespost sind nur akzeptabel, wenn für sie durch Bundesrecht gleichwertige Regelungen geschaffen werden.

Als Sanktionen für etwaige Verstöße gegen diese Vorschriften erscheinen Bußgeldvorschriften ausreichend. Jedoch sollte der § 354 StGB um ein spezielles „Bildschirmtextgeheimnis" erweitert werden.

Der Vorschlag der Datenschutzbeauftragten knüpft an die im Dezember 1980 in Berlin beschlossenen Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)[8] an und berücksichtigt die in der Zwischenzeit bei den Versuchen in Nordrhein-Westfalen und Berlin gewonnenen Erkenntnisse. Der Regelungsvorschlag sollte in seinem wesentlichen Gehalt - soweit sich nicht aus den Begleituntersuchungen zusätzliche Anforderungen ergeben - unverändert in den Staatsvertrag übernommen werden, um Gefahren für das Persönlichkeitsrecht künftiger Teilnehmer durch den Gebrauch von Bildschirmtext soweit wie möglich zu vermeiden.

[8] Jahresbericht 1981, Anlage 3

Die den Ministerpräsidenten vorgelegte Fassung des Staatsvertrages folgt diesen Vorschlägen im wesentlichen, enthält allerdings einige entscheidende Abweichungen:

Während nach dem Vorschlag der Datenschutzbeauftragten die Übermittlung von Abrechnungs- und Verbindungsdaten an Dritte unzulässig sein sollte, sieht die derzeitige Fassung des Staatsvertrages vor, daß diese Daten an Anbieter übermittelt werden dürfen, soweit dies zur Beitreibung von Forderungen erforderlich ist. Dies bedingt die von den Datenschutzbeauftragten abgelehnte Speicherung von personenbezogenen Daten über die Inanspruchnahme einzelner Angebote (wenn auch in einer Form, die Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit der Inanspruchnahme nicht erkennen läßt).

Nicht aufgenommen wurde die Verpflichtung der Anbieter, die Teilnehmer über Speicherung und Übermittlung der von ihm (etwa im Rahmen eines Bestelldienstes) erhobenen Daten zu informieren. Eine solche Aufklärung ist aber unabdingbare Voraussetzung für die erforderliche Einwilligung des Betroffenen.

Schließlich wurde die von den Datenschutzbeauftragten geforderte Kontrollkompetenz beim Betreiber nicht festgeschrieben. Dies führt unter Umständen dazu, daß - angesichts der beschränkten Kontrollbefugnisse im privaten Bereich - eine durchgängige, begleitende Kontrolle der Einhaltung von Datenschutzvorschriften nicht gewährleistet ist. Nach wie vor erscheint es mir geboten, auch in diesen Punkten die Stellungnahme der Datenschutzbeauftragten zu berücksichtigen.

Neben der endgültigen Einführung von Bildschirmtext steht in Berlin in nächster Zeit der Beginn des „Kabelpilotprojektes Berlin" an. Tausend Haushalten im Erprobungsbereich (Schlangenbader Straße) sollen eine Reihe von zusätzlichen Fernseh- und Hörfunkprogrammen (einschließlich eines von den Bürgern mitzugestaltenden Programms), aber auch kommunikativen Diensten (Informations-, Spiel-, Lern- u. ä. Angebote) zur Verfügung gestellt werden. Die Trägerschaft soll in den Händen einer hierfür zu gründenden GmbH liegen.

Zur Beratung bei der Durchführung des Kabelprojektes, insbesondere aber auch zur Erarbeitung eines Medienerprobungsgesetzes für die Erprobung eines umfassenderen Kabelfernsehsystems hat der Senator für Wissenschaft und Kulturelle Angelegenheiten eine Expertenkommission berufen, als deren Mitglied ich frühzeitig die erforderlichen datenschutzrechtlichen Aspekte einbringen kann. Mein Hauptaugenmerk liegt neben der Erarbeitung materieller Regelungen darauf, die öffentliche Kontrolle auch im Bereich des Datenschutzes sicherzustellen.

Erfahrungen mit Bildschirmtext

Auch in diesem Jahr habe ich verfolgt, ob den schutzwürdigen Belangen der Teilnehmer durch die Ausgestaltung von Informationsangebot und Technik bei Bildschirmtext hinreichend Rechnung getragen wurde.

So wurde festgestellt, daß im Wege des Ausprobierens von Zifernfolgen Namen und Anschriften von Versandhauskunden festgestellt werden konnten. Angeblich war es auch möglich, festzustellen, ob der Kunde von diesem Versandhaus gekauft hat. Nach Auffassung der für einen Anbieter zuständigen Aufsichtsbehörde lag hierin zwar kein Verstoß gegen Datenschutzbestimmungen, wenn auch meines Erachtens bessere Sicherungen wünschenswert wären.

Es stellte sich jedoch etwas anderes heraus: Nach der derzeitigen Rechtslage stellt das „Testen" solcher Zufallszahlen einen unbefugten Abruf von Daten dar und erfüllt den Straftatbestand des § 41 Abs. 1 Bundesdatenschutzgesetz; eine mangelnde technische und organisatorische Sicherung wäre jedoch nicht durch eine Sanktionsandrohung geschützt. Dies führt zu der unbefriedigenden Konsequenz, daß sich nicht derjenige strafbar macht, der Daten unzureichend sichert, sondern derjenige, der einen solchen Mangel aufdeckt.

Nicht nur die Programmkonzeption des Anbieters kann Sicherungsmängel aufweisen. Auch technische Schwachstellen des Bildschirmtextsystems eröffnen Möglichkeiten zum Datenmißbrauch.

So hatte eine technisch versierte Person ein Modem (Verbindungselement zwischen Telefonapparat und Btx-Komponenten)

so verändert, daß sie in den Verarbeitungsbereich einer anderen Person eindringen konnte. Sie konnte unter fremdem Namen kostenpflichtige Seiten für mehrere hundert DM aufrufen. Um zu verhindern, daß durch Modemmanipulationen oder andere Maßnahmen bei einzelnen Teilnehmern ein hoher Schaden entsteht, sollte der Teilnehmer die Möglichkeit erhalten, einen Geldbetrag je Tag einzugeben, der das Benutzungslimit darstellt.

In einem weiteren Fall war es möglich, das Angebot eines Anbieters ohne dessen Wissen zu verändern.

Die Möglichkeit, daß unbefugt Dienste abgerufen und Transaktionen vorgenommen werden, ist davon abhängig, welche Sicherheit die verwendeten Kenn- und Geheimzahlen bieten. Richtungweisend ist der Bankverkehr über Bildschirmtext. Hier wird das eigene Konto außer durch verschiedene Kennwörter dadurch geschützt, daß von den Banken Transaktionsnummern eingeführt wurden, die sich nach jedem Buchungsvorgang entsprechend einer dem Teilnehmer ausgehändigten Liste ändern.

Auch diese Codes schützen nicht davor, daß fremde Bildschirmtextaktivitäten durch „Anzapfen" verfolgt werden: Ein augenfälliges Beispiel wäre das Verfolgen des Bankverkehrs eines anderen Teilnehmers. Die mangelnde Abstrahlsicherheit von Fernsehgeräten sowie der relativ leichte Zugang zu Leitungen etwa über die Zusammenführung im Hausverteiler wären Ansatzpunkte für derartige Mißbrauchsmöglichkeiten.

Daß die Rechtspolitik mit der fortschreitenden technischen Entwicklung noch nicht Schritt hält, zeigt auch der im Juni 1982 vorgelegte Gesetzentwurf der Bundesregierung zur Bekämpfung der Wirtschaftskriminalität[9]. Der Entwurf enthält Vorschläge zur Verbesserung des strafrechtlichen Schutzes bei Computerbetrug (§ 263 a Strafgesetzbuch) sowie der Fälschung und mißbräuchlichen Verwertung gespeicherter Daten (§ 269 ff.). Bereits in meinem letzten Jahresbericht[10] habe ich die Frage aufgeworfen, ob nicht auch ein verbesserter strafrechtlicher Schutz vor der mißbräuchlichen Beschaffung und Aufbewahrung von Berechtigungsmerkmalen („Codes") geschaffen werden sollte, um den zu erwartenden Bankverkehr über Bildschirmtext besser zu schützen.

Eine entsprechende Regelung fehlt im Entwurf jedoch.

2.3 Öffentliche Sicherheit und Strafverfolgung

Landesmeldegesetz

§ 23 Melderechtsrahmengesetz[11] verpflichtet die Länder, ihr Melderecht innerhalb von zwei Jahren nach dem Inkrafttreten dieses Gesetzes (am 23. August 1980) den Vorschriften dieses Gesetzes anzupassen. In drei Bundesländern wurden Meldegesetze verabschiedet. Von den übrigen Ländern, zu denen auch Berlin gehört, konnte diese Frist nicht eingehalten werden.

Ein Vorentwurf zu einem Gesetz über das Meldewesen wurde mir im Oktober 1981 zugeleitet. Noch im gleichen Jahr habe ich dazu eine ausführliche Stellungnahme abgegeben. Dabei habe ich betont, daß entsprechend den Intentionen des Melderechtsrahmengesetzes aus der Sicht des Datenschutzes von folgenden Grundpositionen auszugehen sei:

1. Im Gegensatz zu früheren Entwürfen zu einem Bundesmeldegesetz und in Abkehr von früheren Plänen, im Rahmen der sogenannten „Verwaltungsintegration" ein umfassendes Einwohnerinformationssystem mit vielfältigen Datenverknüpfungen der verschiedensten Verwaltungsbereiche zu schaffen, ist nunmehr die gesetzliche Aufgabe der Meldebehörde auf die Identifizierung und Feststellung der Wohnung beschränkt.
2. Die diesbezüglichen Aufgaben sind einer gegenüber anderen Verwaltungseinheiten funktional abgegrenzten Stelle zu übertragen (Meldebehörde), die unabhängig von ihrer organisatorischen Einbindung als abgegrenzte speichernde Stelle zu betrachten ist.
3. Die Weitergabe von Daten von der Meldebehörde an andere Stellen (auch innerhalb derselben organisatorischen Einheit) stellt datenschutzrechtlich eine Datenübermittlung dar.
4. Jede Nutzung der personenbezogenen Daten, die im Melderegister gespeichert werden (sollen) - einschließlich der Erhebung - bedarf der ausdrücklichen Rechtsgrundlage.

Diese Grundpositionen erfordern eine Modifikation der sehr stark auf vollzugspolizeiliche Bedürfnisse zugeschnittenen traditionellen Konzeption des Berliner Meldewesens. Auch der mir vorgelegte Vorentwurf beachtete - auch im Vergleich zu entsprechenden Entwürfen in anderen Ländern - diese den Belangen der Einwohner entsprechenden Positionen nicht hinlänglich.

Von meinen zahlreichen Verbesserungsvorschlägen seien folgende besonders herausgehoben:

Der Vorentwurf erklärte den Polizeipräsidenten in Berlin zur Meldebehörde. Demgegenüber habe ich darauf hingewiesen, daß der durch das Melderechtsrahmengesetz vorgegebene funktional eigenständige Charakter der Meldebehörde auch im Gesetz zum Ausdruck kommen sollte. Insbesondere muß auf diese Weise klargestellt werden, daß die Weitergabe personenbezogener Daten durch die Meldebehörde (d.h. die Meldestellen oder das zentrale Einwohnermeldeamt) auch an andere Polizeidienststellen eine den Datenschutzgesetzen unterworfene Datenübermittlung darstellt.

Neben den Meldedaten selbst gestattet das Melderechtsrahmengesetz die Speicherung sogenannter „Hinweise". Nach der Begründung sollen darunter verstanden werden „Urkunden und andere Nachweise mit Bezeichnung der ausstellenden Behörde oder des Gerichts mit Aktenzeichen und dem Tag der Ausstellung oder des Ereignisses und Angaben über die Rechtswirksamkeit von Änderungen".

Überprüfungen anhand des derzeit noch betriebenen Melderegisters haben gezeigt, daß in diesem Zusammenhang nicht nur Verweise auf die entsprechenden Beweismittel, sondern auch der Inhalt des Beweismittels gespeichert werden. So werden derzeit beim Vorliegen von Wahlausschlußgründen nicht nur die Tatsache des Wahlausschlusses und das Aktenzeichen der entsprechenden Gerichtsentscheidung vermerkt, sondern auch der Grund, der zum Wahlausschluß geführt hat (z.B. „geistige Gebrechlichkeit im Wirkungskreis Vermögensangelegenheiten").

Diese extensive Auffassung der Berechtigung zur Speicherung von Hinweisen führt zur Speicherung von Daten, deren Sensitivität unter Umständen weit über die der im Melderechtsrahmengesetz vorgegebenen Daten hinausgeht. Ihre Verwendung sollte daher im Meldegesetz beschränkt werden.

Auch zum Umfang der personenbezogenen Daten, die über die Vorgabe des Melderechtsrahmengesetzes hinaus gespeichert werden sollen, habe ich Bedenken angemeldet. Die Speicherung folgender Merkmale im Melderegister halte ich nicht für erforderlich: Seriennummer des Passes oder Personalausweises, rechtliche Eigenschaft eines Minderjährigen als Pflegekind, Beruf, Name und Anschrift des Wohnungsgebers. Bei anderen Daten sind Klarstellungen erforderlich (Wahldaten, Religionszugehörigkeit, Mitteilungsersuchen).

Der Vorentwurf sieht die Zulässigkeit eines Ordnungsmerkmals für das Einwohnerregister vor. Ich habe darauf hingewiesen, daß die Erforderlichkeit eines solchen Ordnungsmerkmales zwar beim heutigen Stand der Informationstechnik nicht mehr so deutlich wie bei der herkömmlichen Datenverarbeitung ist, habe die Verwendung eines solchen Ordnungsmerkmales für interne Zwecke jedoch vorläufig nicht in Frage gestellt.

Etwas anderes gilt für die Übermittlung des Ordnungsmerkmals. Die auch vom Rechtsausschuß des Deutschen Bundestags geteilte herrschende Meinung geht davon aus, daß die Einführung eines von örtlichen und sachlichen Zuständigkeiten unabhängigen Personenkennzeichens, das die Verknüpfung jedweder Datenbestände innerhalb und außerhalb der öffentlichen Verwaltung ermöglicht, einen unzulässigen Eingriff in die Persönlichkeitsrechte der Einwohner darstellen würde und verfassungswidrig wäre. Die im Entwurf vorgesehene Zulässigkeit der Übermittlung des Ordnungsmerkmales an andere Behörden erscheint aus diesem Grund unzulässig. Die Verwendung des Ordnungsmerk-

[9] Entwurf eines zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität Bundesrat Drucksache 219/82 vom 4. Juni 1982

[10] S. 14

[11] BGBl. I S. 1429

males sollte deshalb auf die internen Zwecke beschränkt und jegliche Übermittlung ausgeschlossen werden.

Der Entwurf sieht eine – mit Bußgeldandrohung bewehrte – Nebenmeldepflicht des Wohnungsgebers vor. Ich habe bezweifelt, daß die Nebenmeldepflicht des Wohnungsgebers überhaupt erforderlich ist, denn eine wirksame Verbesserung der Qualität des Melderegisters ist hierdurch kaum zu erwarten. Unvertretbar ist jedoch die Nebenmeldepflicht hinsichtlich des Auszugs aus der Wohnung. Diese setzt voraus, daß der Wohnungsgeber (der häufig räumlich entfernt vom Meldepflichtigen wohnt) eine ständige Kontrolle des Mieters vornimmt. Unproblematisch ist diese Pflicht ohnehin nur in den Fällen, in denen nach wirksamer Kündigung ein Auszug erfolgt. Dies werden aber gerade die Fälle sein, in denen der Meldepflichtige selbst seine Abmeldung bzw. Anmeldung bei der neuen Wohnung vornimmt und auf die die Nebenmeldepflicht gerade nicht zielt.

Der Entwurf sieht vor, daß bei Zweifeln über die Person des Meldepflichtigen in der Meldebehörde erkennungsdienstliche Maßnahmen auch gegen seinen Willen durchgeführt werden können. Diese in keinem anderen Entwurf für ein Landesmeldegesetz vorgesehene Regelung ist ein besonders deutliches Beispiel für die Vorrangigkeit polizeilicher Zielsetzungen bei der Abfassung des Entwurfs.

Die Durchführung erkennungsdienstlicher Maßnahmen (insbesondere wenn sie zwangsweise erfolgt) und die damit verbundene Aufbewahrung der aus der Maßnahme entstandenen Unterlagen stellt einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Sie ist grundsätzlich nur bei Gefahren für die Sicherheit und Ordnung sowie für die Strafverfolgung hinnehmbar[12]. Der Vollzug des Meldegesetzes stellt keine Aufgabe dar, die für sich allein die Vornahme solcher Maßnahmen rechtfertigt.

In ähnlich auffälliger Weise rückt die bereits im derzeitigen Melderecht bestehende Verpflichtung der Inhaber von Beherbergungsstätten, Gäste innerhalb von 24 Stunden nach ihrem Eintreffen bei der Meldebehörde zu melden, polizeiliche Gesichtspunkte in den Vordergrund. Diese Vorschrift läßt beim Polizeipräsidenten eine vollständige Datei sämtlicher Gäste entstehen, die in Berlin beherbergt werden. Dieser Umfang erscheint unverhältnismäßig und nicht erforderlich, zumal auch in den Musterentwürfen für ein Meldegesetz die Bereithaltung der Meldescheine für die Polizei für ausreichend erklärt wurde. Ich habe empfohlen, daß auch in Berlin die Meldescheine von den Beherbergungsstätten nur bereitgehalten, nicht aber täglich der Polizei übergeben werden sollen. Die Verpflichtung, eine namentlich zu meldende Person bei der Meldebehörde anzuzeigen, wenn sie das Ausfüllen des Meldescheins oder die Unterschrift verweigert, verpflichtet die Leiter von Beherbergungsstätten in unverhältnismäßigem Umfang zum Zusammenwirken mit der Meldebehörde und den Sicherheitsbehörden. Zur Durchsetzung scheint ausreichend, Verstöße als Ordnungswidrigkeiten zu ahnden.

Der Entwurf sieht vor, daß in Krankenanstalten ein Verzeichnis aller Patienten zu führen ist. Dieses Verzeichnis ist der Meldebehörde auf Verlangen vorzulegen. Für Zwecke der Gefahrenabwehr und der Strafverfolgung sowie für die Aufklärung der Schicksale von Vermißten und Unfallopfern sollen die Daten (durch die Polizei) ausgewertet und verarbeitet werden dürfen.

Ich habe demgegenüber vertreten, daß Daten über den Aufenthalt in Krankenhäusern medizinische Daten sind, die einem gesteigerten Geheimhaltungsinteresse und entsprechend auch der ärztlichen Schweigepflicht unterliegen. Die undifferenzierte Ermächtigung zur Verarbeitung dieser Daten zu den vorgegebenen Zwecken ist zwar vom Melderechtsrahmengesetz vorgegeben, unterliegt aber verfassungsrechtlichen Bedenken. So habe ich darauf hingewiesen, daß das Bundesverfassungsgericht entschieden hat, daß ein Eingriff in die Privatsphäre des Bürgers durch die Einsichtnahme in medizinische Daten nicht generell mit dem Interesse an der Aufklärung von Straftaten gerechtfertigt werden kann, sondern daß vielmehr *überwiegende* Belange des Gemeinwohls dies zwingend gebieten müssen[13]. Die Übermittlung dieser Daten an die Meldebehörde ist in keinem Fall gerechtfertigt und auch durch § 16 Abs. 3, 4 Melderechtsrahmengesetz nicht gedeckt: Dort ist bestimmt, daß nur an diejenigen Stellen Daten übermittelt werden dürfen, die mit der Aufgabe der Gefahrenabwehr und der Strafverfolgung usw. betraut sind. Ähnliche Bedenken gegen die Bestimmung hat der Senator für Gesundheit, Soziales und Familie erhoben.

Soweit vorgesehen ist, den Zugriff auf das Melderegister mit Hilfe von On-line-Anschlüssen zu ermöglichen, habe ich vorgeschlagen, der Zulässigkeit solcher Anschlüsse die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entwickelten Grundsätze zugrunde zu legen. Dieser Vorschlag wurde in der Parlamentsvorlage bereits berücksichtigt.

Für die parlamentarische Beratung des Entwurfs habe ich diese Gesichtspunkte nochmals in einer gesonderten Stellungnahme zusammengefaßt, die ich den Fraktionen zum 1. Dezember 1982 zugeleitet habe.

Meldewesen

Auch das auf dem bisherigen Meldegesetz von 1970 beruhende Verfahren warf einige rechtliche und tatsächliche Probleme auf. Eine Vielzahl von Bürgern machte von ihrem Recht Gebrauch, gem. § 13 Abs. 1 Berliner Datenschutzgesetz Auskunft über die zu ihrer Person gespeicherten Daten sowie über die Empfänger der nicht regelmäßigen Übermittlungen der letzten zwei Jahre zu verlangen. Dabei kam es zeitweise zu erheblichen Bearbeitungszeiten. Die Ursache lag darin, daß der Polizeipräsident für die Auskunft über die Übermittlungen der letzten zwei Jahre eine Programmänderung durch die zur technischen Konzeption der Einwohnerdatenbank eingerichtete „Projektgruppe Einwohnerwesen" veranlassen mußte, da die vorhandenen Programme nur für Einzelanfragen geeignet waren. Dieses Beispiel zeigt, daß Ansprüche, die im Berliner Datenschutzgesetz dem Bürger eingeräumt werden, nicht immer in hinreichender Weise in entsprechende technische Konzepte umgesetzt werden.

Schwierigkeiten macht auch die Umsetzung der Vorschriften, die die sogenannte „einfache Melderegisterauskunft" regeln: Nach § 17 a Meldegesetz darf anderen Personen als den Betroffenen ohne Nachweis bestimmter Voraussetzungen Auskunft über Namen, akademische Grade und Anschriften einzelner bestimmter Personen erteilt werden. Fraglich ist, wann eine Person derart bestimmt ist. So hatte sich eine Petentin darüber beschwert, daß ihre Adresse einem Dritten übermittelt worden sei, der eine Person mit gleichem Namen, aber abweichendem Geburtsdatum suchte. Zwar hatte der Auskunftsersuchende das Geburtsdatum genannt, da im Melderegister zu jener Zeit aber nur eine Person mit dem betreffenden Namen registriert war, wurde auf die Abweichung des Geburtsdatums keine Rücksicht genommen und die Auskunft nur im Hinblick auf den Namen erteilt. Dieser Fall wird zum Anlaß genommen, mit dem Polizeipräsidenten Gespräche über eine neue Festlegung der Abfragekriterien zu führen.

Eine Diskrepanz zwischen den Vorstellungen des Bürgers und den Intentionen des Datenschutzes zeigt sich an folgendem Fall: Ein Petent, der aufgrund seines Namens besonders häufig mit anderen Personen verwechselt wurde, hatte einen Antrag auf Namensänderung gestellt und die Namensänderung erreicht. Er beschwerte sich, daß trotz der Berichtigung im Melderegister auch nach der Namensänderung wiederholt Verwechselungen im Zusammenhang mit seinem Kraftfahrzeug auftraten. Er vertrat die Auffassung, daß die zum Melderegister gemeldete Namensänderung ohne weitere Maßnahmen auch an alle anderen Dateien zumindest beim Polizeipräsidenten hätte gemeldet werden müssen.

Diese Vorstellung setzt eine Verknüpfung von Dateien aus verschiedenen Verwaltungsbereichen voraus, die aus unterschiedlichen Gründen datenschutzrechtlichen Bedenken begegnet. Die Einrichtung entsprechender Meldedienste würde die Schaffung einer Vielzahl neuer Informationsflüsse bedeuten und damit einer Vernetzung der verschiedensten Verwaltungsbereiche den Weg bereiten. Auf diese Weise würde, insbesondere durch den Einsatz automatischer Datenverarbeitungsanlagen eine Transparenz des Bürgers hergestellt, die dem verfassungsrechtlich fundierten Grundsatz, die freie Entfaltung der Persönlichkeit zu gewährleisten, widersprechen würde.

[12] Vgl. §§ 81 b, 161 b StPO, 16 ASOG

[13] BVerfGE 32, 380 f

Kraftfahrzeugfahndung

In einer Eingabe beschwerte sich ein Bürger, daß er an einem westdeutschen Grenzübergang angehalten worden war, weil sein Fahrzeug nicht versichert sei. Tatsächlich bestand seit längerer Zeit bereits wieder ein korrekter Versicherungsschutz. Meine Nachforschungen ergaben, daß eine Fahndung nach dem Fahrzeug für kurze Zeit ausgelöst worden war, daß die Löschungsverfügung des Kraftverkehrsamtes (Referat Ord D des Polizeipräsidenten) wohl die Kfz-Datei, nicht jedoch die Kfz-Fahndungsdatei des INPOL-Systems erreicht hatte. Um die Wiederholung dieses Fehlers auszuschließen, habe ich empfohlen, die Ordnungsmäßigkeit des Verfahrens dadurch zu verbessern, daß die dem Referat Ord D als der für die Richtigkeit der Daten materiell zuständigen Stelle durch entsprechende Rückmeldungen die Richtigkeit der Eintragungen in die Kfz-Fahndungs-Datei kontrollierbar gemacht wird. Der Polizeipräsident ist zwischenzeitlich meiner Empfehlung gefolgt.

Feuerwehr

Datenschutzrechtliche Fragen wurden im vergangenen Jahr auch im Bereich der Berliner Feuerwehr aufgeworfen.

Im Zusammenhang mit den Bemühungen, sowohl die Einsatzleitung als auch die Gebührenabrechnung zu automatisieren, entstand die Frage, ob der Berliner Feuerwehr ein On-line-Zugriff auf den Bestand des Melderegisters eröffnet werden sollte. Gegen einen derartigen Direktzugriff spricht die derzeitige Rechtslage: § 10 Berliner Datenschutzgesetz läßt eine Datenübermittlung zwischen öffentlichen Stellen nur zu, wenn diese zur Aufgabenerfüllung erforderlich ist; bei einem On-line-Anschluß gilt aber die Gesamtmenge der zum Abruf bereitgehaltenen Daten als übermittelt[14]. Die Kenntnis der Gesamtmenge der Daten der Einwohnerdatei ist jedoch für die Aufgaben der Berliner Feuerwehr nicht erforderlich.

Angesichts dieser Rechtslage habe ich empfohlen, den diesbezüglichen Teil des Sollkonzepts bis zum Abschluß des Gesetzgebungsverfahrens zu dem Landesmeldegesetz zurückzustellen: Dort kann auf dem Wege spezialgesetzlicher Regelungen die Zulässigkeit von On-line-Zugriffen neu geregelt werden. Dies ist aufgrund meiner Empfehlungen auch beabsichtigt.

Schwer zu lösen ist eine Kollision zwischen dem Interesse an einer schnellen Krankenversorgung und dem Datenschutz im Rahmen der von der Berliner Feuerwehr durchgeführten Krankentransporte. Um den Kranken möglichst schnell in ein auch fachlich geeignetes Krankenhaus einliefern zu können, hat die Feuerwehrleitzentrale ein großes Interesse an der (vorläufigen) Diagnose des eingesetzten Notarztes, zum anderen verlangen die Krankenkassen im Zusammenhang mit der Kosteneinziehung von der Feuerwehr auf den Krankentransportbescheinigungen die Angabe der Diagnose des Aufnahmearztes. Die ärztliche Schweigepflicht gebietet, daß eine Übermittlung personenbezogener Daten ohne Einwilligung nur zum Schutz eines höheren Rechtsgutes oder im Rahmen der aufeinander folgenden Behandlung durch mehrere Ärzte erfolgt[15]. Während dies im Zusammenhang mit der Einlieferung in ein geeignetes Krankenhaus hingenommen werden kann, gilt dies nicht für die Mitteilung der Diagnose an die Krankenkasse.

Ein Problem der Zusammenarbeit zwischen Feuerwehr, Polizei und speichernder Stelle war in Zusammenhang mit einem Brand in einer Bankfiliale zu erörtern. Betroffene hatten sich darüber beschwert, daß die Feuerwehr bei einer Brandbekämpfung Bankauszüge und andere Datenträger auf die Straße geworfen und unbewacht zurückgelassen habe. Auf diese Weise hätten eine Vielzahl personenbezogener Daten von Bankkunden durch Passanten eingesehen werden können. Meine aufgrund der Beschwerde eingeleiteten Ermittlungen ergaben folgendes: Während des Löscheinsatzes gebührt der Entfernung brennbarer Materialien aus dem Brandbereich der Vorrang. Die geborgenen Gegenstände einschließlich etwaiger vorhandener Datenträger werden außerhalb des Gefahrenbereiches abgelegt und der Bewachung durch die Polizei unterstellt. Diese informiert ihrerseits den (die speichernde Stelle vertretenden) Verantwortlichen des in Brand geratenen Betriebes. Dieser hat dann für die Sicherung der auf den Datenträgern enthaltenen Daten zu sorgen. Wenn auch der Beschwerdefall zeigt, daß dieses Verfahren nicht immer zu einer hinreichenden Sicherung führt, gehe ich davon aus, daß jedenfalls von Seiten der beteiligten Behörden ein angesichts der Gefahrensituation angemessener Datenschutz gewährleistet ist.

Strafverfolgung

Ungeachtet der Sachleitungsbefugnis der Staatsanwaltschaft bei der Strafverfolgung liegt die Ermittlungstätigkeit auf diesem Gebiet im wesentlichen in Händen der Polizei, in Berlin beim Dezernat Verbrechensbekämpfung der Landespolizeidirektion, den Referaten Verbrechensbekämpfung der Polizeidirektionen sowie der Direktion Spezialaufgaben der Verbrechensbekämpfung. Daneben sind weitere Dienststellen mit der Strafverfolgung befaßt, insbesondere die Abschnitte, die mit der Entgegennahme von Anzeigen beauftragt sind.

Für die Erfüllung der Aufgaben dieser Dienststellen ist die Führung von „Kriminalpolizeilichen personenbezogenen Sammlungen" (KpS) erforderlich, aus denen einerseits Informationen über Straftaten und Tatverdächtige, andererseits über Anzeigeerstatter, Opfer und Zeugen hervorgehen. Die hohe Sensibilität dieser Daten erfordert große Sorgfalt bei der Führung der Datensammlungen und die Aufmerksamkeit aller für den Datenschutz Verantwortlichen.

Die KpS lassen sich in drei Gruppen aufteilen:

Das traditionelle Arbeitsmittel der Kriminalpolizei ist die Kriminalakte, in der die zu einer Person angefallenen und nach Abgabe des Vorgangs an die Staatsanwaltschaft zurückbehaltenen Vorgänge personenorientiert aufgenommen werden. In der Regel ohne Rücksicht auf anderweitig (z.B. im Bundeszentralregistergesetz) festgelegte Tilgungsfristen sind traditionellerweise hier alle Personen erfaßt, die – ohne Rücksicht auf die staatsanwaltschaftliche oder richterliche Bestätigung – im Verdacht gestanden haben, eine Straftat begangen zu haben. Diese Kriminalakten werden in Berlin an zentraler Stelle aufbewahrt und können für Zwecke der Strafverfolgung, aber auch für andere Zwecke der öffentlichen Verwaltung zur Verfügung gestellt werden.

Der Aktenzugriff ist seit einigen Jahren durch das „Informationssystem für Verbrechensbekämpfung" (ISVB) erleichtert. Mit Hilfe einer Vielzahl von Datenendgeräten (Kleinrechner mit Druckern, Bildschirmgeräte, Fernschreiber) kann von den einzelnen Dienststellen aus u.a. festgestellt werden, ob zu bestimmten Personen Kriminalakten existieren und ob aktuelle Ermittlungsvorgänge in Bearbeitung sind. Zusätzlich übernimmt dieses System weitere Funktionen, die die traditionelle Führung der Kriminalakten nicht oder nur beschränkt leistete: Nachweis der aktuellen Sachbearbeitung (auch in bezug auf einzelne Anzeigeerstatter und Geschädigte), Nachweis von Fahndungsnotierungen und taktischen Hinweisen (etwa „gefährlicher Gewaltverbrecher"), Beschreibung von Tatmerkmalen und Datenverbund mit dem Bundeskriminalamt und den anderen Landeskriminalämtern über das sogenannte INPOL-Verbundsystem.

Das ISVB macht die Führung zusätzlicher manueller Datensammlungen nicht überflüssig. Vielmehr erweist sich für die Arbeit einzelner Kriminaldienststellen, vor allem besonders spezialisierter Einheiten, die Führung sogenannter „Arbeitskarteien" als erforderlich. Sie enthalten in der Regel nur eine sehr begrenzte Anzahl relevanter Daten, die die für die unmittelbare Arbeit von Kriminaldienststellen erforderlichen Daten in speziell zugeschnittener Form zur Verfügung stellen.

Die Art und Weise, wie alle diese Datensammlungen geführt werden, stand bislang im freien Ermessen der Polizeidienststellen. Insbesondere gab es keine allgemein verbindlichen Regelungen über die Dauer der Aufbewahrung der Unterlagen sowie die Auskunft über die Unterlagen an die Betroffenen. Einen erheblichen Fortschritt aus datenschutzrechtlicher Sicht haben hier die „Richtlinien für die Führung Kriminalpolizeilicher personenbezoger Sammlungen" (KpS-Richtlinien) gebracht, die in Berlin mit Erlaß vom 15. April 1981 eingeführt wurden. In den vergangenen eineinhalb Jahren konnten eine Reihe von Erfahrungen mit den Richtlinien gewonnen werden, die insgesamt gesehen zeigen, daß

[14] § 4 Abs. 2 Ziff. 2 Berliner Datenschutzgesetz
[15] § 2 Berufsordnung der Ärztekammer Berlin

eine Reihe datenschutzrechtlich relevanter Probleme hier in durchaus angemessener Form geregelt wurde.

Wenn auch die Richtlinien keinen formellen Gesetzescharakter haben und damit für die Bürger nur bedingte Rechte geschaffen wurden, besteht kein Zweifel daran, daß die Polizei im großen und ganzen um die konsequente Umsetzung der in den Richtlinien enthaltenen Grundgedanken bemüht war.

Daß dabei noch nicht alle Probleme gelöst sind, mögen folgende Beispiele belegen:

Die in KpS enthaltenen Daten gehen weit über den Umfang der Daten hinaus, die im Bundeszentralregister gespeichert werden. Im Gegensatz zu den dort enthaltenen Strafregisterdaten, denen stets ein durch Staatsanwaltschaften oder Gerichte abgeschlossenes Verfahren zugrunde liegt und die nach genau festgesetzten Fristen getilgt oder mit Auskunftsbeschränkung (zu tilgende Verurteilungen) versehen werden, sind hier über erheblich längere Zeiträume auch Daten aus unbestätigten Verdächtigungen vorhanden. Da nach der Zwecksetzung des Bundeszentralregisters dieses das vorrangige Auskunftsmittel über strafrechtliche Vorwürfe ist, müssen Auskünfte an Dritte aus KpS weitgehenden Beschränkungen unterliegen. So bestimmt Ziff. 3.6 der KpS-Richtlinien, daß Mitteilungen über im Bundeszentralregister getilgte oder zu tilgende Verurteilungen und die zugrundeliegenden Straftaten an andere als Polizeidienststellen unterbleiben, falls nicht besondere Ausnahmetatbestände vorliegen. Das Bundeszentralregistergesetz fordert hierzu, daß eine Berücksichtigung solcher Taten nur stattfinden darf, wenn sonst eine erhebliche Gefährdung der Allgemeinheit zu gewärtigen wäre. Die Überprüfung einzelner Eingaben zeigte, daß das Vorliegen einer solchen erheblichen Gefährdung nicht immer hinreichend streng überprüft wurde. So wurden 1981 und 1982 noch Übermittlungen über Verdächtigungen aus dem Jahre 1963 festgestellt.

Die Übermittlung derartiger Angaben widerspricht auch den in den KpS-Richtlinien vorgesehenen Regeln über die Aussonderung von Unterlagen. Danach sind im Sinne einer verallgemeinernden Interessenabwägung Unterlagen regelmäßig dann auszusondern, wenn bei den Betroffenen zehn Jahre lang die Voraussetzungen für eine Aufnahme von Erkenntnissen in die KpS nicht vorlagen. Eine solche Aussonderung ist nicht nur im Rahmen besonderer Aussonderungsaktionen, sondern auch dann vorzunehmen, wenn die Unterlagen im Rahmen einer Bearbeitung (z.B. eines Auskunftsersuchens) zum Vorschein kommen („Anlaßaussonderung"). Vom Polizeipräsidenten wurde in Aussicht gestellt, daß insbesondere im Zusammenhang mit der Auskunftserteilung an dritte Stellen ein Verfahren gefunden werden soll, das gewährleistet, daß auszusondernde Aktenbestandteile keine Verwertung mehr finden. Künftig kann die elektronische Datenverarbeitung hier Hilfestellung bieten, indem automatisch Listen mit auszusondernden Unterlagen gefertigt werden.

Besondere Probleme stellt die ebenfalls von den KpS-Richtlinien vorgesehene Aussonderung von Unterlagen in den Fällen, in denen Entscheidungen der Staatsanwaltschaft oder eines Gerichts ergeben, daß die Gründe, die zur Aufnahme in die KpS geführt haben, nicht zutreffen. Dies trifft in erster Linie für Entscheidungen zu, in denen der Tatvorwurf durch Freispruch oder auf andere Weise entkräftet wird. Eine konsequente Durchführung einer solchen Aussonderung stößt nach Angaben des Polizeipräsidenten deswegen auf Schwierigkeiten, weil die hierzu erforderlichen Rückmeldungen von Justizbehörden nicht in dem erforderlichen Umfang erbracht werden können. Erfahrungen in anderen Ländern zeigen jedoch, daß hierfür Verfahren entwickelt werden konnten, die auch in Berlin eingeführt werden sollten.

Eine wesentliche Errungenschaft der KpS-Richtlinien stellt die Regelung dar, daß dem Betroffenen aus den KpS Auskunft darüber zu erteilen ist, ob und ggf. welche Unterlagen zur Person in den KpS vorhanden sind, es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen. Im Berichtszeitraum haben zahlreiche Bürger von dieser Möglichkeit Gebrauch gemacht. In den weitaus meisten Fällen erteilte die Polizei die erwünschten Auskünfte.

Von dem Vorbehalt wurde insbesondere dann Gebrauch gemacht, wenn es sich um Gewohnheitstäter, besonders schwere Straftaten oder laufende Ermittlungen handelte. Auf meine Empfehlung hin wird nunmehr der Grund der Auskunftsverweigerung jedenfalls in den Fällen den Betroffenen mitgeteilt, in denen diesen der zugrundeliegende Sachverhalt bekannt ist.

Problematisch bleibt die Erfüllung des Anliegens, Ausforschungsversuche zu verhindern, die auch dann nicht ausgeschlossen sind, wenn in den KpS keine Eintragung vorhanden ist. Der Polizeipräsident hat sich im Einvernehmen mit dem Innensenator entschlossen, dem dadurch vorzubeugen, daß aufgrund einer schematischen Abfolge bei einzelnen Auskunftsersuchen grundsätzlich keine Auskunft erteilt wird. Dieses Verfahren ist noch Gegenstand von Gesprächen mit dem Senator für Inneres.

Gegen Ende des Berichtszeitraumes wurde damit begonnen, das Informationssystem für Verbrechensbekämpfung einer datenschutzrechtlichen Überprüfung zu unterziehen. Im Vordergrund des Interesses steht insbesondere die Frage, auf welche Weise durch eine differenzierte Ausgestaltung der Zugriffsberechtigungen sichergestellt werden kann, daß ein Zugriff auf die gespeicherten Daten, insbesondere aber eine Veränderung der gespeicherten Daten nur durch die zuständigen Stellen bzw. Sachbearbeiter vorgenommen werden kann. Zwar ist hier ein absoluter Schutz nicht zu gewährleisten; dies zeigen Gerichtsverfahren, in denen Polizeibeamten der Abruf von Daten zu privaten Zwecken vorgeworfen wurde. Durch hinreichende technische und organisatorische Maßnahmen können derartige Vorkommnisse jedoch weitgehend verhindert werden.

Über die im ISVB vorgesehenen formalen Zugriffsbeschränkungen sollten zusätzliche Beschränkungen in Abhängigkeit vom Dateninhalt vorgenommen werden. So erscheint mir erforderlich, daß der Zugriff auf Daten von Kindern und Jugendlichen, Opfern von Denunziationen, psychisch Kranken u.a. auf das für kriminalpolizeiliche Zwecke unumgängliche Maß beschränkt wird.

In den nächsten Jahren wird hierüber hinaus verstärkt die Problematik der Vernetzung kriminalpolizeilicher Informationssysteme mit anderen Datenbanken (Kriminalaktennachweis beim Bundeskriminalamt, Einwohnerdatenbank, Kraftfahrzeugregister u.ä.) zu diskutieren sein.

Aufgrund einer Reihe von Eingaben bestand schließlich Anlaß, die Arbeitskarteien der mit Sexualstraftaten befaßten Kommissariate in der Direktion Spezialaufgaben für Verbrechensbekämpfung in Augenschein zu nehmen. Dabei bestätigte sich, daß der von Homosexuellen mitunter geäußerte Verdacht, die Polizei speichere nach wie vor personenbezogene Daten auch solcher Homosexueller, die keiner heute noch strafbaren Handlung verdächtigt werden, nicht zutrifft. Nach der Liberalisierung des Sexualstrafrechts im ersten Strafrechtsänderungsgesetz wurden die vorhandenen Arbeitskarteien, die der Ermittlung und Identifizierung von Sexualstraftätern dienen, bereinigt.

Kriminalpolizeiliche personenbezogene Sammlungen im Zusammenhang mit Hausbesetzungen

Aufgrund verschiedener Eingaben sowie entsprechender Forderungen in der Öffentlichkeit führte ich eine Überprüfung sämtlicher personenbezogener Daten durch, die im Zusammenhang mit Hausbesetzungen vom Polizeipräsidenten erhoben, gespeichert und übermittelt wurden. In die Überprüfung wurden auch die Staatsanwaltschaft bei dem Landgericht sowie das Landesamt für Verfassungsschutz einbezogen. Mit Schreiben vom 29. April 1982 wurde dem Senator für Inneres ein umfangreicher Bericht über die Ermittlungsergebnisse überreicht.

Der Bericht enthielt keine abschließende datenschutzrechtliche Bewertung, sondern zunächst nur die Aufzählung einzelner Datenverarbeitungsvorgänge, die aus der Sicht des Datenschutzes Bedenken hervorriefen. Im wesentlichen bezogen sich die Bedenken darauf, daß personenbezogene Daten sämtlicher in die Ermittlung einbezogener Personen unabhängig von Anlaß und Art der Erhebung Gegenstand undifferenzierter Datenübermittlungen sowie entsprechender Datenspeicherungen bei den Adressaten wurden. Beteiligt sind hierbei außer verschiedenen Polizeidienststellen das Landesamt für Verfassungsschutz, Verfassungsschutzämter im Bund und anderen Ländern sowie das Bundeskriminalamt.

Eine Stellungnahme des Senators für Inneres ist erst am 1. November 1982 eingegangen. Ich kann eine endgültige datenschutzrechtliche Bewertung erst abgeben, wenn die sich daraus ergebenden Fragen geklärt sind.

Anordnung der Veröffentlichung von Verurteilungen in der Tagespresse

Bei bestimmten Straftatbeständen, der Beleidigung (§§ 185 ff. StGB) und der „falschen Verdächtigung" (§ 164 StGB) ist unter besonderen Voraussetzungen auf Antrag des Verletzten oder des zur Stellung eines Strafantrags Berechtigten die öffentliche Bekanntgabe der Verurteilung vom Gericht anzuordnen (§§ 165 und 200 StGB).

Entsprechende Veröffentlichungen in der Berliner Tagespresse haben in mehreren Fällen zu Anfragen von Bürgern geführt, ob diese Praxis gegen das Datenschutzrecht verstoße.

Für die Zulässigkeit dieses Verfahrens spricht die eindeutige, spezialgesetzliche Regelung im Strafgesetzbuch. Veränderungen der Regelung fallen in die Zuständigkeit des Bundesgesetzgebers. Problematisch erscheint, daß dem Richter vom Gesetz keinerlei Handlungs- und Beurteilungsspielraum eingeräumt wird. Auf Antrag hat er wie ein „Urteilsautomat" die Veröffentlichung anzuordnen. De lege ferenda wäre zu erwägen, ob dem Richter nicht ein Entscheidungsspielraum eingeräumt werden sollte. Die Entscheidung könnte an die Schwere der Tat und die Form der Verbreitung falscher Angaben gebunden werden. Auf diese Weise könnte vermieden werden, daß jede anläßlich einer Festnahme gemachte Äußerung zum Abdruck der Verurteilung in einer Berliner Tageszeitung führen würde.

Das Problem wird vor allem dadurch verschärft, daß in Berlin eine Anordnung vorliegt, wonach bei Beleidigung von Polizisten dieser Antrag generell von der Dienststelle gestellt werden soll. Ich habe mich bemüht, eine Modifizierung dieser Regelung zu erreichen, so daß nur in Einzelfällen - je nach der Schwere der Tat und der Form der Verbreitung falscher Angaben - vom Antragsrecht Gebrauch gemacht wird. Dies wurde vom Polizeipräsidenten abgelehnt.

Ich habe den Bundesdatenschutzbeauftragten auf dieses Problem aufmerksam gemacht.

2.4 Sozialwesen

Im Berichtsjahr hat sich bestätigt, daß den seit 1. Januar 1981 geltenden Vorschriften über den Schutz der Sozialdaten im 2. Kapitel des Sozialgesetzbuches - Zehntes Buch - (SGB X) erhebliche Bedeutung zukommt. Weite Bereiche der öffentlichen Verwaltung erbringen heute Sozialleistungen und müssen den Umgang mit personenbezogenen Daten daher nicht nur mit den Datenschutzgesetzen, sondern nunmehr auch mit dem SGB X in Einklang bringen.

Der Vollzug der neuen Vorschriften fällt den Verwaltungen nicht immer leicht. Dies liegt zum einen an der Kompliziertheit der Regelungen; zum anderen beschneiden die Vorschriften aber auch Informationsflüsse, die bislang üblich waren und teilweise nach wie vor für zweckmäßig gehalten werden. So kam es im Berichtsjahr erneut zu einer Reihe mir bekannt gewordener Verstöße gegen das SGB X auch in den Fällen, auf die ich im Jahresbericht 1981 bereits hingewiesen hatte.

Aus diesem Grunde soll auf wesentliche Offenbarungstatbestände nochmals eingegangen werden.

Offenbarung für die Erfüllung sozialer Aufgaben (§ 69 SGB X)

Die für die Sozialverwaltung bedeutendste Vorschrift ist § 69 SGB X. Hiernach ist die Offenbarung personenbezogener Daten insbesondere zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch einen Sozialleistungsträger erforderlich ist, auch dann, wenn die Offenbarung gegenüber einer nicht-öffentlichen Stelle erfolgen soll.

Im einzelnen ist die Beurteilung der Erforderlichkeit nicht einfach.

Die schon in meinem Jahresbericht 1981 angesprochene Frage nach der Zulässigkeit der Angabe des Überweisungsgrundes auf Überweisungsträgern ist auch in diesem Jahre von Bedeutung gewesen. Ich habe Beschwerden von Bürgern erhalten, bei denen der Überweisungsgrund für Sozialhilfe so weit aufgeschlüsselt war, daß aus dem Überweisungsträger Angaben erkenntlich waren wie „Reparatur von Schuhsohlen und Absätzen, Reinigung eines Wintermantels, Kauf einer Haushaltsleiter etc.". Mag es auch problematisch sein, auf die Angabe des Überweisungsgrundes völlig zu verzichten, so meine ich doch, daß eine derart weitreichende Offenbarung keinesfalls erforderlich ist.

Ich hoffe, daß die Bemühungen, auf die Angabe des Überweisungsgrundes zu verzichten, auch im kommenden Jahr fortgeführt werden. Ich begrüße die auf der 23. Arbeitstagung der Aufsichtsbehörden der Sozialversicherungsträger getroffene Feststellung, im Bereich der Krankenversicherung darauf hinzuwirken, daß die Versicherten die ihnen zustehenden Leistungen auch ohne vollständige Offenbarung des Leistungsgrundes erhalten sollen.

Im Ergebnis zielt meine Auffassung dahin, die Daten auf Überweisungsträgern soweit wie möglich zu reduzieren. Dabei sollten automatisierte Verfahren schrittweise so ausgestaltet werden, daß der Überweisungsträger auf einen - ggf. automatisch erstellten Bescheid - Bezug nimmt, der dem Bürger getrennt zugeht.

Mehrere Beschwerden richteten sich dagegen, daß in den Fällen, in denen die Sozialhilfe nicht bar, sondern mit Hilfe von Kostenübernahmescheinen geleistet wird, den Einzelhändlern nicht nur die Tatsache, daß Sozialhilfe geleistet wird, sondern auch der Name des Sozialhilfeempfängers bekannt wird.

Diese Praxis ist nicht zu beanstanden. Der Sozialleistungsträger kann die Art der Sozialleistung selbst bestimmen, die Verwendung von Kostenübernahmescheinen kann insbesondere zur Verhütung von Mißbrauch angezeigt sein; in diesem Falle ist aber auch die Offenbarung der in Frage stehenden Daten in bestimmtem Umfang als erforderlich anzusehen.

Die Erforderlichkeit für die Aufgabenerfüllung steht dann in Frage, wenn es ohne größere Schwierigkeiten möglich ist, vor der Offenbarung die Einwilligung des Betroffenen einzuholen. Die damit verbundenen Abwägungsschwierigkeiten seien an folgendem Beispiel erläutert:

Im Rahmen der Sozialhilfe werden auch Kosten für Elektrizität und Gas übernommen. Da der Verbrauch nur einmal jährlich abgelesen wird, im übrigen nur Pauschalzahlungen geleistet werden, ist es häufiger zu einem unverhältnismäßig hohen Energieverbrauch durch Sozialhilfeempfänger gekommen. Ein derartiger Mißbrauch von Sozialleistungen kann frühzeitig festgestellt werden, wenn in Verdachtsfällen eine monatliche Ablesung vorgenommen wird. Dies setzt aber die Übermittlung personenbezogener Daten an die Energieversorgungsunternehmen voraus.

Datenschutzrechtlich wäre folgende Regelung optimal:

Vor der Datenübermittlung wird der Betroffene aufgefordert, seine Einwilligung zur Übermittlung der Daten an die Energieversorgungsunternehmen zu geben. Die Verpflichtung zur Einwilligung ergibt sich aus § 60 SGB I. Wird die Einwilligung nicht erteilt, kann die Sozialleistung entzogen werden; zwar würde dies in einem späteren Stadium doch die Übermittlung von Sozialdaten bedingen (hier: Nichterteilung der Einwilligung mit den entsprechenden Konsequenzen gem. § 66 SGB I), der Betroffene erhält aber auf diese Weise vor der Übermittlung Kenntnis davon und kann sich entsprechend einstellen. Zudem gib es gesetzliche Gründe, die den Betroffenen zur Verweigerung der Mitwirkung berechtigen (§ 65 SGB I).

Auf der anderen Seite ist zu berücksichtigen, daß der Sozialhilfeberechtigte nur Anspruch auf den notwendigen Lebensunterhalt hat, so daß die Mitteilung von Sozialdaten an die Energieversorgungsunternehmen insoweit „erforderlich" sein könnte. In diesem Fall gestattet § 69 Abs. 1 Ziff. 1 SGB X die Offenbarung auch ohne Einwilligung des Betroffenen.

Da die erste Lösung einen geringeren Eingriff als die zweite darstellt, wäre ihr - gerade unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes - der Vorzug zu geben.

In Übereinstimmung mit einem entsprechenden Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder bin ich zu der Auffassung gelangt, daß bei folgendem Sachverhalt dagegen § 69 Abs. 1 keine Anwendung finden kann und somit eine unzulässige Offenbarung von Sozialdaten vorliegt:

Nach § 1 Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht sind in Berlin die Bezirksämter für die Befreiung zuständig. Die Befreiung von den Rundfunkgebühren selbst wird nicht in einem besonderen Buch des SGB geregelt, stellt mithin keine Aufgabe nach § 69 Abs. 1 dar. Andererseits entnehmen die Bezirksämter für die Gebührenbefreiung die erforderlichen Angaben den ihnen vorliegenden Sozialakten und übermitteln die Gründe auf bundeseinheitlichen Formularen an die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu beschlossen:

Sind die Gemeinden zur Entscheidung über die Gebührenbefreiungspflicht allein zuständig, dürfen die Rundfunkanstalten keine unter das Sozialgeheimnis fallenden personenbezogenen Daten erhalten, da sie zur Aufgabenerfüllung nicht erforderlich sind. Es genügt die Mitteilung der Tatsache der Gebührenbefreiung. Dies gilt auch für die Datenweitergabe an die GEZ. Die statistischen Auswertungen der GEZ können auch ohne personenbezogene Meldungen durchgeführt werden.

Offenbarung für die Erfüllung besonderer gesetzlicher Mitteilungspflichten (§ 71 SGB X)

Hauptproblem beim Vollzug von § 71 SGB X ist der in Ziff. 2 geregelte Informationsaustausch zwischen Sozial- und Ausländerbehörden. Danach ist die Übermittlung von Sozialdaten an Ausländerbehörden nur zum Schutz der öffentlichen Gesundheit zulässig. Dem steht gegenüber, daß ein Ausländer ausgewiesen werden kann, wenn er den Lebensunterhalt für sich und seine unterhaltsberechtigten Angehörigen nicht ohne Inanspruchnahme der Sozialhilfe bestreiten kann oder bestreitet (§ 10 Abs. 1 Ziff. 10 Ausländergesetz). Die für diese Entscheidung notwendigen Informationen wurden vor Inkrafttreten des SGB X, in vielen Fällen aber auch noch danach durch die Sozialbehörden beigebracht[16]. Die Rechtslage wurde vielfach als unbefriedigend empfunden und führte auch in diesem Jahr zu einer Reihe von fragwürdigen Verfahren.

Um den Belangen des § 120 Bundessozialhilfegesetz Rechnung zu tragen, wurde gelegentlich vor der Gewährung von Sozialhilfe von den Sozialämtern eine Anfrage an die Ausländerbehörde gerichtet, ob dort Erkenntnisse vorliegen, die der Gewährung von Sozialhilfe entgegenstehen können. Wenngleich dabei die Ausländerbehörde erfuhr, welcher Ausländer Sozialhilfe beantragt hat, habe ich dieses Verfahren nicht beanstandet, da die Sozialbehörden verpflichtet sind, die Leistungsvoraussetzungen zu prüfen.

Anläßlich einer anderen Beschwerde wurde mir die Praxis bekannt, die Zahlung der Sozialhilfe von der Abgabe einer Einwilligungserklärung zur Datenübermittlung an die Ausländerbehörde abhängig zu machen. Aufgrund einer Eingabe beim Petitionsausschuß veranlaßte der Senat, die Bezirksämter erneut mit Nachdruck auf die Beachtung der datenschutzrechtlichen Vorschriften und der in diesem Zusammenhang erlassenen Verwaltungsvorschriften aufzufordern. Er wies zusätzlich darauf hin, daß eine nach § 67 SGB X einzuholende schriftliche Einwilligung des Betroffenen zur Offenbarung seiner personenbezogenen Daten in der deutschen und in seiner Muttersprache inhaltlich übereinstimmen und den Hinweis enthalten müsse, daß ihm keine Nachteile erwachsen, wenn er von der Möglichkeit, das Einverständnis zu verweigern, Gebrauch macht[17].

In Zusammenhang mit der Ergänzung des SGB X um ein drittes Kapitel wurde in diesem Jahr auf Veranlassung der Länder § 71 SGB X geändert: Nunmehr wurde ein Offenbarungstatbestand für den Datenaustausch zwischen Ausländer- und Sozialbehörden geschaffen. Die neue Vorschrift erstreckt sich auch auf die Fälle, in denen ein Ausländer in Täuschungsabsicht unrichtige oder keine Angaben macht sowie in denen dessen Anwesenheit erhebliche Belange der Bundesrepublik Deutschland beeinträchtigt (§ 71 Abs. 2 SGB X neue Fassung).

Auch die für die Wehrüberwachung zuständigen Stellen wurden in den Kreis der Berechtigten einbezogen (§ 71 Abs. 1 Ziff. 4 SGB X neue Fassung).

Offenbarung für die Durchführung eines Strafverfahrens (§ 73 SGB X)

§ 73 SGB X enthält bestimmte Voraussetzungen für die Offenbarung von Sozialdaten zu Zwecken der Strafverfolgung. Danach setzt die Offenbarung eine richterliche Anordnung voraus. Liegt die richterliche Anordnung vor, dürfen zur Aufklärung eines Verbrechens alle personenbezogenen Daten, zur Aufklärung eines Vergehens lediglich Vor- und Familienname, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften des Betroffenen, Namen und Anschriften seiner derzeitigen und früheren Arbeitgeber sowie Angaben über erbrachte oder demnächst zu erbringende Geldleistungen offenbart werden.

An mich ist die Frage herangetragen worden, ob neben dieser Spezialvorschrift die allgemeine Amtshilfevorschrift des § 68 SGB X anwendbar ist, die zwar die Herausgabe eines beschränkten Datensatzes (Vor- und Familienname, Geburtsdatum, Geburtsort, derzeitige Anschrift, Name und Anschriften seines derzeitigen Arbeitgebers) zuläßt, die Einholung einer richterlichen Anordnung aber entbehrlich macht. Unter Berufung auf diese Vorschrift hatte sich die Polizei vielfach an Sozialleistungsträger mit der Bitte um die Übermittlung personenbezogener Daten gewandt und hierzu auch ein entsprechendes Formblatt entwickelt.

Im Gegensatz zu der von der Polizei vertretenen Auffassung ist davon auszugehen, daß die allgemeine Amtshilfe nicht in Frage kommt, wenn eine besondere Offenbarungsvorschrift für einzelne Tatbestände ein spezielles Verfahren vorschreibt. Damit scheidet jedenfalls für den Bereich der Strafverfolgung die Anwendbarkeit von § 68 aus. Für die Fälle, in denen die Polizei nicht zur Strafverfolgung, sondern im Rahmen anderer Aufgaben (z.B. Gefahrenabwehr, Vollzug von Haftbefehlen) tätig wird, kann die Offenbarung auf § 68 gestützt werden.

Ich habe in Übereinstimmung mit dem für Grundsatzfragen des Sozialgesetzbuches zuständigen Senator für Arbeit und Betriebe eine entsprechende Änderung des von der Polizei verwendeten Formulars vorgeschlagen.

Von Bedeutung war diese Problematik bei einem Strafverfahren, in dem ein Mitarbeiter eines Arbeitsamtes wegen Strafvereitelung (§ 258 StGB) angeklagt wurde: Ein Angestellter hatte der Polizei auf deren Anfrage hin mitgeteilt, ein gesuchter Arbeitsloser befinde sich gerade im Dienstgebäude. Da die Polizei keine richterliche Anordnung vorweisen konnte, hielt ein Mitarbeiter diese Mitteilung für unzulässig und schickte den Arbeitslosen weg.

Nachdem die erste Instanz ihn zu einer Geldstrafe verurteilt hatte, da dem Strafverfolgungsanspruch der Vorrang einzuräumen sei, sprach ihn das Berufungsgericht frei. Dieser Fall, der in der Öffentlichkeit einiges Aufsehen erregte, hat auch im Bereich der Berliner Verwaltung zu einer Verunsicherung darüber geführt, inwieweit Sozialbehörden auskunftspflichtig sind.

Dessenungeachtet ergibt die derzeitige Rechtslage, die nur durch eine Gesetzesänderung auf Bundesebene modifiziert werden kann. Auch der Aufenthalt in einer Sozialdienststelle ist dann (und nur dann) vom Sozialgeheimnis geschützt, wenn sich durch zusätzliche Kenntnisse der Bezug zur Gewährung von Sozialleistungen herstellen läßt. Dementsprechend ist die Offenbarung eines solchen Datums nur unter den geschilderten gesetzlichen Voraussetzungen zulässig.

Offenbarung für die Forschung oder Planung (§ 75 SGB X)

§ 75 SGB X gestattet unter bestimmten Voraussetzungen die Offenbarung von Sozialdaten auch im Rahmen öffentlicher und privater Forschung. Eine wichtige Voraussetzung für die Zulässig-

[16] Vgl. Jahresbericht 1981, S. 12

[17] Vgl. die Antwort des Senats auf die Kleine Anfrage Nr. 1085, Drucksache 9/651, S. 46

keit ist die Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde, in Berlin je nach Geschäftsbereich insbesondere die Senatoren für Arbeit und Betriebe sowie für Schulwesen, Jugend und Sport. Durch frühzeitige Information, mitunter auch durch die Mitwirkung beim Genehmigungsverfahren hatte ich Gelegenheit, die datenschutzrechtlichen Aspekte der Forschungsvorhaben zu begutachten und beratend tätig zu werden. So wurden Forschungsprojekte über Obdachlosigkeit, über die Lebensbewältigung Jugendlicher aus der Jugendhofarbeit oder über delinquente junge Ausländer genehmigt.

Welche Schwierigkeiten bei derartigen Forschungsprojekten bestehen können, sei an folgendem Beispiel illustriert:

Von der Arbeitsgemeinschaft für Sozialberatung und Psychotherapie wurde in Zusammenarbeit mit den Jugendämtern ein Forschungsprojekt zur Jugendverwahrlosung geplant. Die privatrechtlich organisierte, jedoch im Auftrag und unter Aufsicht der Bezirksämter handelnde Arbeitsgemeinschaft benötigt die Einsicht in die Akten der Pflegekinder bei Jugendämtern, um einerseits die Beratung der Pflegeeltern im Rahmen des Forschungsprojektes durchführen und andererseits personenbezogene Daten der Pflegekinder während der Begleituntersuchung verwerten zu können. Die Zulässigkeit dieses Projektes richtet sich nach §§ 27 Abs. 1 SGB I, 4 Jugendwohlfahrtsgesetz, wonach die Jugendämter ihre Aufgaben in Zusammenarbeit mit den Trägern der freien Jugendhilfe oder der Arbeitsgemeinschaft erfüllen.

Da die Beratung der Eltern für die Betreuung der Kinder auch zur Erfüllung des Pflegeverhältnisses erforderlich ist, war die Akteneinsicht in dieser Hinsicht als zulässig zu beurteilen. Personen oder Stellen, denen hierbei personenbezogene Daten offenbart werden, unterliegen nach § 78 SGB X der Zweckbindung und Geheimhaltungspflicht, d.h. sie dürfen die Daten nur zu dem Zweck verwenden, zu dem sie ihnen befugt offenbart worden sind.

Die Offenbarung von personenbezogenen Daten für die wissenschaftliche Auswertung und Begleituntersuchung ist dagegen nach § 75 SGB X zu beurteilen. Das zusätzliche Genehmigungserfordernis ist im Hinblick auf die in § 78 SGB X enthaltene und durch das Forschungsprojekt durchbrochene Zweckbindung gerechtfertigt.

Zweckbindung und Geheimhaltungspflicht des Empfängers (§ 78 SGB X)

§ 78 SGB X bestimmt, daß Empfänger von Sozialdaten diese nur zu dem Zweck verwenden dürfen, zu dem sie sie erhalten haben. Insoweit unterliegen sie der gleichen Geheimhaltungspflicht wie die Sozialleistungsträger.

Eine interessante Fallkonstellation zu dieser Bestimmung wurde mir im Rahmen eines Beratungsvorganges vorgelegt:

Die Apothekerkammer hatte bei der Aufsichtsbehörde nachgefragt, ob es datenschutzrechtlich zulässig sei, daß in Apotheken mit Hilfe von Datenverarbeitungsanlagen aus den Verordnungsblättern der gesetzlichen Krankenkassen (Rezepte) folgende Daten gespeichert werden:

1. Persönliche Daten wie Name, Vorname, Geburtstag, Geschlecht, Anschrift und verordnete Arzneimittel von Versicherten sowie
2. Name, Vorname, Berufsbezeichnung, Anschrift, Kassenarztnummer, Telefonnummer und Arzneimittelumsätze von einzelnen Kassenärzten zu speichern.

Diese Daten könnten zu Werbezwecken und zur Kontrolle und Beeinflussung von Umsatzdaten der Ärzte sowie zum Arzneimittelverbrauch der Patienten verwendet werden.

Diese Anfrage warf schwierige Rechtsfragen des Sozialversicherungsrechtes als Vorfragen auf. Im Ergebnis ergibt sich aus den Vorschriften der Reichsversicherungsordnung, des Bundesmantelvertrages der Ärzte und des Gesamtvertrages der Krankenkassen mit dem Berliner Apothekerverein, daß die Verordnungsblätter im Rahmen der zwischen den Landesapothekervereinen und den Krankenkassen bestehenden Lieferverträge verwendet werden. Der Arzt trägt die Daten „für die Krankenkassen" auf die Verordnungsblätter ein. Den Apothekern werden daher Sozialdaten der Krankenkassen offenbart, deren Rechtmäßigkeit sich nach §§ 78, 69 Abs. 1 Nr. 1 SGB X bestimmt. Die Offenbarung ist nur zulässig, soweit sie zur Erfüllung der Aufgaben der Krankenkassen erforderlich ist. Der Apotheker darf die Daten nur zu dem Zweck verwenden, zu dem sie ihm befugt offenbart worden sind. Eine darüber hinausgehende Speicherung ist nach § 78 SGB X unzulässig.

Geltung des Bundesdatenschutzgesetzes (§ 79 SGB X)

Zu den Schwierigkeiten beim Vollzug des SGB X trägt bei, daß *Landes*behörden, die Aufgaben nach dem Sozialgesetzbuch wahrnehmen, gleichwohl *Bundes*datenschutzrecht anwenden müssen. Hierzu gehört, daß im Bereich der Sozialverwaltung nach den §§ 28, 29 Bundesdatenschutzgesetz behördliche Datenschutzbeauftragte zu benennen sind, während eine solche Verpflichtung für andere Behörden in Berlin (etwa im Gegensatz zu Bayern) nicht besteht.

Der Datenschutzbeauftragte hat nach § 29 Bundesdatenschutzgesetz wichtige Aufgaben zu erfüllen. So hat er neben seiner allgemeinen Kontrollaufgabe eine Übersicht über die Art der gespeicherten personenbezogenen Daten (internes Dateienregister) zu führen, die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Erfordernissen des Datenschutzes vertraut zu machen und bei der Auswahl dieses Personenkreises beratend mitzuwirken.

Im Gegensatz zu den Senatsverwaltungen und den Körperschaften im Sozialleistungsbereich fand sich ein Teil der Bezirksämter erst nach eindringlichen Beratungen bereit, einen Datenschutzbeauftragten zu benennen.

Eine weitere Frage in diesem Zusammenhang war deshalb zu klären, weil der Bundesrechnungshof die Auffassung vertreten hatte, der Leiter der Revisionsabteilung einer öffentlichen Körperschaft könne mit den Aufgaben eines Datenschutzbeauftragten nicht betraut werden, da dies der Ausschließlichkeit der Aufgabenzuweisung an die Revisionsstellen widerspreche.

In Berlin hatte die Landesversicherungsanstalt den Leiter der Revisionsabteilung zum Datenschutzbeauftragten ernannt. Hierzu habe ich geltend gemacht, daß ich aus dem Blickwinkel des Datenschutzes der Benennung von Mitarbeitern aus diesem Bereich schon deswegen keine Bedenken entgegenbringe, weil im Rahmen der Überprüfung der Ordnungsgemäßheit der Datenverarbeitung ohnehin eine Vielzahl von Datenschutzaspekten mitgeprüft werden muß.

Rechtsentwicklung

Das SGB X ist im Berichtsjahr um ein drittes Kapitel ergänzt worden, in dem die Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten geregelt werden. Dieses Kapitel ist deshalb datenschutzrechtlich relevant, weil hier Außenstehenden Auskunftspflichten auferlegt werden (z. B. Arbeitgebern, Angehörigen, Unterhaltsverpflichteten und Ärzten), die den für sie geltenden Datenschutzgesetzen vorgehen und Befugnisnormen darstellen, die auch Amts- und Berufsgeheimnisse verdrängen.

Gegen den Vorentwurf dieser Ergänzung hatten die Datenschutzbeauftragten deswegen Bedenken geltend gemacht, weil künftig ärztliche Untersuchungsmaßnahmen oder psychologische Eignungsuntersuchungsmaßnahmen so durchgeführt werden sollen, daß sie auch bei der Prüfung der Voraussetzung anderer Sozialleistungen verwendet werden können. Die Datenschutzbeauftragten hatten befürchtet, daß diese Bestimmung zum Anlaß für die Bildung einer Zentraldatei genommen werden könnte, in der verzeichnet ist, welche Gutachten von den verschiedenen Leistungsträgern angefordert worden sind.

Den Bedenken wurde nunmehr dadurch Rechnung getragen, daß die Bildung einer solchen Zentraldatei für nicht zulässig erklärt wird (§ 102 Abs. 3 SGB X).

Auf weitere Detailänderungen des SGB X, die im Laufe dieses Jahres in Kraft traten, wurde an anderer Stelle hingewiesen.

3. Kontrolle organisatorischer und technischer Datenschutzmaßnahmen

3.1 Grundsatzfragen

Veränderte Anforderungen auf Grund der technischen Entwicklung

Trends in der Entwicklung der Informationstechnik werden durch die ständige Verbesserung der Zykluszeiten, Hauptspeichergrößen, Packungsdichten und Übertragungsgeschwindigkeiten belegt. Damit wird zugleich der schnelle technologische Fortschritt der Mikroelektronik dokumentiert.

Am praktischen Einsatz von Informationstechnik läßt sich jedoch ein anderer, nicht minder bedeutsamer Trend erkennen: Die Datenverarbeitung konzentriert sich nicht mehr auf ein relativ abgeschlossenes Rechenzentrum. Die für die bisherige Technologie charakteristische Trennung von Arbeitsplatz und Computer wird durch das deutlich zu beobachtende Bestreben, die automatische Datenverarbeitung in das Arbeitsfeld des Sachbearbeiters einzubeziehen, abgelöst. Die dabei entstehenden neuen Kommunikationswege schaffen eine immer umfassendere Infrastruktur der Datenverarbeitung. Diese Entwicklung wird durch die Integration von Nachrichten- und Datenübertragungsmedien mit moderner Technologie zur Datengewinnung, -erfassung, -speicherung und -verarbeitung gefördert. Sie bestimmt die einschlägigen Messen und die Verkaufspolitik der Hersteller. Die Neuen Medien durchbrechen mittlerweile als sogenannte „offene", d. h. jedermann zugängliche Systeme sogar die Organisationsgrenzen, die auch der automatischen Datenverarbeitung bisher in aller Regel gezogen sind.

Systeme, die Sachbearbeitern auch über große Entfernungen hinweg Zugang zu zentralen Datenbeständen verschaffen und Verfahren, die die Datenfernübertragung durch selbständige Einrichtungen zwischen verschiedenen Systemen erlauben, sind mittlerweile Standard einer zunehmenden Zahl moderner größerer ADV-Anwendungen geworden. Diese On-line-Systeme und -Anschlüsse sind eine Vorstufe der genannten Infrastruktur.

Für den Datenschutzbeauftragten bedeutet dies, daß er sich in seinen Beratungs- und Kontrollfunktionen auf diese technische Entwicklung einstellen muß. Dies gilt auch für seine Kontrolltätigkeit hinsichtlich der technisch-organisatorischen Maßnahmen, die nach § 5 Berliner Datenschutzgesetz erforderlich sind, um den Datenschutz zu gewährleisten. Durch diese Maßnahmen soll erreicht werden, daß Daten nur jene erreichen, die mit ihnen umgehen sollen, und daß die Möglichkeit zur vorsätzlichen oder versehentlichen, jedenfalls unzulässigen Offenbarung von geschützten Daten soweit möglich und angemessen verhindert wird.

Die Anforderungen an die Kontrolle organisatorischer und technischer Maßnahmen zum Datenschutz haben sich mit den verbesserten Möglichkeiten zum dezentralen Zugriff auf Datenbestände und Programme verändert. Den Schwerpunkt einer Kontrolle bildet nicht mehr nur die Überprüfung des unmittelbaren Bereichs des Rechenzentrums, sondern vielmehr die Beobachtung von Informationsflüssen in der gesamten Organisation.

Dies ist auch durch ein anderes Phänomen begründet: Die organisatorische und technische Sicherung von Datenbeständen und Datenträgern ist eine Anforderung, der sich die unmittelbar mit der Datenverarbeitung Beschäftigten schon lange zu stellen hatten. Das Bewußtsein dafür ist deshalb insbesondere bei Rechenzentrumsleitern und Operateuren wesentlich ausgeprägter als bei Mitarbeitern anderer Organisationsbereiche, die erst im Zuge der neueren technologischen Entwicklung mit dem Problem konfrontiert werden.

Bei meiner Prüftätigkeit - besonders bei organisatorischen Fragen - habe ich außerdem die Erkenntnis berücksichtigen müssen, daß in den der eigentlichen automatischen Datenverarbeitung vor- und nachgelagerten manuellen Be- und Verarbeitungsprozessen von Daten wesentliche Risiken verborgen sind.

Diese Erfahrungen haben die Entwicklung meines Prüfkonzeptes bestimmt, nachdem in diesem Jahr in mehreren Fällen vorgegangen wurde.

Traditionelle Verwaltung und moderne Datenverarbeitung

Die Verwaltungsstrukturen sind Ergebnis einer langen Entwicklung. Die Informationsflüsse innerhalb der Verwaltung, vor allem zwischen verschiedenen Ressorts, sind wesentlicher Bestandteil dieser Strukturen. Der Einsatz von modernen ADV-Verfahren, insbesondere die zentral gesteuerte Verwendung von Datenbanken und Informationssystemen, hat die Organisation der Informationsflüsse unter erheblichen Anpassungsdruck gesetzt, da diese modernen Verfahren nicht als einzelne Elemente, sondern bereits als neue Infrastrukturen anzusehen sind.

Die Verwaltung hat die Anpassung an die moderne Informationstechnik dadurch geleistet, daß sie häufig eine zusätzliche für die ADV verantwortliche Verwaltungseinheit geschaffen und die Informationsflüsse entsprechend verlängert hat.

Zwei bezeichnende Vorgänge haben mir gezeigt, daß diese Lösung zwar dem Bedarf der eingreifenden Verwaltung nach schnell und zentral verfügbaren Daten in den meisten Fällen befriedigt, daß die Zuverlässigkeit der Datenverarbeitung unter der Verlängerung des Informationsflusses jedoch leiden kann. Denn dadurch wird die Anzahl der Fehlerquellen vergrößert, ohne daß sich der Umfang der Sicherungen erhöht. Da die Informationen, die das Verwaltungshandeln gegenüber dem Bürger bestimmen, zunehmend aus Datenbanken gewonnen werden, besteht die Gefahr, daß die schutzwürdigen Belange des Bürgers stärker beeinträchtigt werden als zuvor, sofern nicht darauf geachtet wird, daß den wachsenden Gefahren entsprechende zusätzliche Sicherungen gegenüberstehen. Die Beispiele hierfür habe ich in den Abschnitten 2.3 und 4 behandelt:

- Daten über Beginn oder Ende von Pflegschaften erreichen die Einwohnerdatenbank nicht immer und führen dann zu Fehlern beim Versand von Wahlunterlagen und in der Wählerliste.
- Daten über die Aufhebung von Kraftfahrzeugfahndungen wegen fehlenden Versicherungsschutzes erreichen die polizeilichen Informationssysteme nicht immer und führen dann zu irrtümlichen Eingriffen von Grenzkontrollstellen.

Ich habe in beiden Fällen angeregt, daß die Verwaltungen, die die Daten erzeugen (Amtsgerichte bzw. Ref. Ord D des Polizeipräsidenten [Kraftverkehrsamt]), in zuverlässiger Weise aktenkundig machen, ob ein Datum letztlich korrekt in die Datenbank eingetragen oder aus ihr gelöscht worden ist. Mir wurde in jedem Falle ein Argument entgegengehalten, welches auf die historisch gewachsenen Verwaltungsstrukturen Bezug nimmt: Die geforderte Rückkoppelung bedeute Kontrolle der ADV-Verwaltung durch dafür unzuständige Instanzen. Erfreulicherweise konnten in beiden Fällen jedoch Verfahren erarbeitet werden, die die Belange des Bürgers besser berücksichtigen. Damit wurde erreicht, daß die Instanz, die ein Datum erzeugt, der Verantwortung für seine Richtigkeit auch bei der späteren Verwendung des Datums gerecht werden kann.

Öffentliche Verwaltung und private EDV-Unternehmen

Die Durchführung von ADV-Projekten in der öffentlichen Verwaltung Berlins wird in der Regel in Zusammenarbeit zwischen der jeweiligen Behörde und dem Landesamt für Elektronische Datenverarbeitung (LED) durchgeführt. Von dieser Regel gibt es jedoch Ausnahmen, in denen Privatunternehmen mehr oder weniger in die Projekte und laufenden Verfahren einbezogen werden.

Zweifellos kann die Zusammenarbeit mit Privatunternehmen eine schnellere, unbürokratischere und häufig auch wirtschaftlichere Bedienung der öffentlichen Stellen mit sich bringen als wenn von Anfang bis Ende verwaltungseigene Kapazitäten eingesetzt würden. Jedoch birgt diese Zusammenarbeit Risiken, die bei der Beachtung der vom LED angewendeten Regelungen - etwa dem Automationshandbuch - vermieden werden können.

So habe ich festgestellt, daß bei einigen kleineren Verfahren eine nicht hinnehmbare Abhängigkeit der öffentlichen Stellen von der Dienstleistungsbereitschaft der privaten Unternehmen entstanden ist. Das gelegentlich geringe Interesse der privaten

Unternehmen, für ausreichende Transparenz ihrer Verfahren zu sorgen und so eine Überprüfbarkeit vor allem durch die anwendende öffentliche Stelle selbst, aber auch durch Kontrollinstanz zu ermöglichen, kann unter Umständen die Einsatzfähigkeit des Verfahrens und damit die Funktionsfähigkeit der öffentlichen Stelle gefährden. Bei der Ausschreibung von Verfahren sind deshalb im Pflichtenheft strenge Maßstäbe an die Dokumentation hinsichtlich ihrer Vollständigkeit und Verständlichkeit zu setzen. Meine Anforderungen entsprechen dabei den Mindestanforderungen der Rechnungshöfe.

Kleinrechner und Textverarbeitungssysteme

Der Einsatz von Kleinrechnern bzw. Textverarbeitungssystemen zur Ver- und Bearbeitung personenbezogener Daten erfolgt häufig auch bei öffentlichen Stellen, die ansonsten noch keine Datenverarbeitung betreiben oder die für einzelne Spezialanwendungen eine solche Anlage unabhängig von einem arbeitsteilig organisierten Rechenzentrumsbetrieb verwenden. Bei solchen Stellen besteht oft Unsicherheit über die technischen und organisatorischen Maßnahmen, die zur Gewährleistung des Datenschutzes auch bei derartigen Systemen erforderlich sind. Zweifellos ist auch hier von dem Grundsatz auszugehen, daß der Aufwand für entsprechende Maßnahmen in einem vernünftigen Verhältnis zum Aufwand für die Datenverarbeitung stehen muß. Dabei ist allerdings zu berücksichtigen, daß personenbezogene Daten auf derartigen Anlagen keiner größeren Gefährdung unterliegen dürfen als in Rechenzentren.

3.2 Stellungnahme zu ADV-Verfahren

Die rechtzeitige Übersendung ausführlicher Unterlagen (insbesondere Hauptuntersuchungsberichte, Pflichtenhefte) über geplante ADV-Verfahren durch die Fachverwaltungen gab mir auch in diesem Jahr Gelegenheit, vor Einrichtung dieser Verfahren aus datenschutzrechtlicher und technisch-organisatorischer Sicht Stellung zu beziehen. Damit hatte ich die Möglichkeit, Probleme aufzugreifen, und mit den Verwaltungen zu klären, bevor Tatsachen geschaffen werden, die nur mit großem Aufwand noch verändert werden können. Insbesondere hinsichtlich der baulichen und technischen Sicherungen bei Rechenzentren und der sicheren organisatorischen Abläufe wurden in verschiedenen Fällen Fragen aufgeworfen, deren genauere Behandlung erforderlich war.

In einigen Fällen wurde ich so rechtzeitig informiert, daß ich noch meine Wünsche für den Fall der Durchführung einer Hauptuntersuchung formulieren und so datenschutzbezogene Aspekte bereits in die Planungsphase einbringen konnte.

Neben den allgemeinen, vorbeugenden Anregungen, die ich in meinen Stellungnahmen geben konnte, waren in einigen Fällen auch besondere Probleme zu behandeln, die einer Erwähnung bedürfen und die noch nicht in allen Fällen abschließend geklärt sind.

Bei der *Amerika-Gedenkbibliothek* soll die computergestützte Ausleihverbuchung eingesetzt werden. Die beim Betrieb der Bibliothek anfallenden personenbezogenen Daten, insbesondere die sogenannten variablen Benutzerdaten, die einen Ausleihvorgang beschreiben, erlauben Rückschlüsse auf individuelle Interessen und sind somit Daten, die als sensitiv einzuschätzen sind. Bei ihrem Mißbrauch können die schutzwürdigen Belange des Benutzers im erheblichen Maße beeinträchtigt werden. Aus diesem Grund ist es datenschutzrechtlich nicht hinnehmbar, daß - wie geplant - die variablen Benutzerdaten nach endgültigem Abschluß eines Ausleihvorganges lediglich gesperrt, nicht jedoch gelöscht werden. Nach § 9 Berliner Datenschutzgesetz ist die Speicherung personenbezogener Daten nur so lange zulässig, wie es zur rechtmäßigen Aufgabenerfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist. Ein Interesse des Betroffenen daran, daß Daten über sein Ausleihverhalten nicht gelöscht, sondern lediglich gesperrt werden, ist nicht erkennbar, ebensowenig weitere Nutzungsmöglichkeiten der gesperrten Daten gemäß § 14 Abs. 2 Berliner Datenschutzgesetz. Ich habe daher gefordert, daß solche Daten gemäß § 14 Abs. 3 Berliner Datenschutzgesetz gelöscht werden.

Der *Senator für Wirtschaft und Verkehr* plant die Einführung einer *Betriebsdatenbank*, die neben der Automatisierung des gewerberechtlichen Benachrichtigungsverfahrens auch zur Verbesserung der wirtschaftspolitischen und planerischen Aufgabenerfüllung dienen soll. Eine Überprüfung der Grundstruktur der geplanten Betriebsdatenbank ergab, daß die Einführung dieses Verfahrens fachlich zu einer Kompetenzverschiebung zu Gunsten des Senators für Wirtschaft und Verkehr und zu Lasten der zuständigen Wirtschaftsämter der Bezirke führen würde. Ich habe deshalb insoweit Bedenken geäußert, als die datenschutzrechtliche Verantwortung in dem Verfahren nicht mehr den tatsächlichen Verhältnissen entspräche. Die Wirtschaftsämter könnten ihrer gesetzlichen Verantwortung nicht mehr in vollem Umfange nachkommen.

Nach § 14 Gewerbeordnung erfolgt die Gewerbeanmeldung beim zuständigen Wirtschaftsamt des Bezirkes. Die Datenübermittlung zwischen Wirtschaftsamt und Senator für Wirtschaft und Verkehr richtet sich nach Nr. 20 Ausführungsvorschriften zu §§ 14, 15 Abs. 1 und 55 c Gewerbeordnung. Der Umfang dieser Übermittlung ist nach § 10 Abs. 1 Berliner Datenschutzgesetz an der Erforderlichkeit der Daten für die Aufgabenerfüllung der empfangenden Stelle zu messen, da eine andere Festlegung des Umfangs nicht besteht.

Nach dem neuen Verfahren soll der Senator für Wirtschaft und Verkehr nun den vollen Datenbestand der Wirtschaftsämter erhalten, da er im Auftrag der Wirtschaftsämter das gewerberechtliche Benachrichtigungsverfahren, das u. a. ihn selbst als Empfänger vorsieht, durchführen soll. Mit dieser Auftragsvergabe begeben sich die Wirtschaftsämter de facto ihrer Möglichkeit, über die Zulässigkeit der Datenübermittlung an den Senator für Wirtschaft und Verkehr zu entscheiden.

Auf der Grundlage eines Alternativvorschlages wurde Einigung über die folgende Modifizierung des Verfahrens erzielt: Sowohl die Auftragsdatenverarbeitung für die Wirtschaftsämter als auch die Verwendung der Betriebsdatenbank für eigene Zwecke kann beim Senator für Wirtschaft und Verkehr stattfinden. Jedoch sollen diese beiden verschiedenen Anwendungen organisatorisch getrennt werden, so daß einerseits den Wirtschaftsämtern die Option erhalten bleibt, die Datenverarbeitung wieder selbst zu übernehmen und andererseits sichergestellt wird, daß der Senator für Wirtschaft und Verkehr die für seine Zwecke benötigten Daten jederzeit in einem On-line-Verfahren erhält.

Die *Berechnung und Nachweisung der Mieten und Umlagenabrechnung* für Grundstücke und Wohnungen im Eigentum des Landes Berlin, die die Grundstücksämter der einzelnen Bezirke durchführen, erfolgt bei der *Wohnungsbau-Rechenzentrum (WBRZ) GmbH* im Auftrag der Bezirksämter. Die WBRZ GmbH ist privatrechtlich organisiert. Meine Kontrollbefugnis ist jedoch gem. § 2 Abs. 3 Berliner Datenschutzgesetz gegeben, da mehr als 50 % der Anteile dem Land Berlin gehören. Dabei kommt es nach § 2 Abs. 3 Berliner Datenschutzgesetz nicht darauf an, daß sich die Höhe der Beteiligung aus Schachtelbeteiligungen ergibt. Dem Umgang mit personenbezogenen Daten der Mieter werde ich besondere Aufmerksamkeit widmen.

3.3 Überprüfung von Rechenstellen

In diesem Jahr konnte ich damit beginnen, öffentliche Stellen nach einem vorbereiteten Konzept auf die organisatorischen und technischen Maßnahmen hin zu überprüfen, die nach § 5 Abs. 1 Berliner Datenschutzgesetz zu treffen sind, um den Datenschutz zu gewährleisten. Diese Überprüfungen erfolgen routinemäßig, d. h. nicht nur aus konkretem Anlaß heraus und sollen nach und nach alle öffentlichen Stellen erfassen. In diesem Jahr habe ich folgende Überprüfungen dieser Art durchgeführt:

- Die Zentrale Vormundschaftskasse/Unterhaltsvorschußkasse des Senators für Schulwesen, Jugend und Sport
- die Deutsche Klassenlotterie Berlin
- das Rudolf-Virchow-Krankenhaus
- das Landesamt für Elektronische Datenverarbeitung, Rechenzentrum Spandau
- das Bezirksamt Zehlendorf von Berlin.

Darüberhinaus wurden kleine Prüfungen zu speziellen Themen aus dem Bereich der technisch-organisatorischen Maßnahmen bei gegebenem Anlaß durchgeführt.

Die Auswertung der Prüfung beim Bezirksamt Zehlendorf ist noch nicht abgeschlossen. Beim Rechenzentrum Spandau des LED wurden zu den geprüften Schwerpunkten bezüglich der technischen und organisatorischen Maßnahmen keinerlei Mängel festgestellt.

Bei den übrigen Stellen habe ich eine Reihe von Mängeln vorgefunden und diese den geprüften Stellen mitgeteilt. Gleichzeitig habe ich Empfehlungen zur Beseitigung dieser Mängel gegeben und bei der Realisierung der Empfehlungen beratend mitgewirkt. Im allgemeinen haben die geprüften Stellen meinen Empfehlungen Rechnung getragen und damit begonnen, die Mängel zu beseitigen.

Mängel in Sicherheitsbereichen
(Rechnerraum, Datenträgerarchiv)

Bei mehreren Stellen habe ich festgestellt, daß Rechnerräume und Archive nicht ausreichend vor unbefugtem Zutritt geschützt waren. Insbesondere war nicht ausreichend restriktiv und verbindlich festgelegt worden, wer Zugang zu diesen Bereichen haben soll und wer nicht. Ein Besucherbuch, welches alle nicht regelmäßig zum Zutritt befugten Personen erfaßt, die den Sicherheitsbereich betreten, wurde in der Regel nicht geführt.

Bei mehreren Stellen habe ich weiterhin festgestellt, daß das Vier-Augen-Prinzip im Rechnerraum keineswegs strikt gewahrt wurde.

Eine räumliche Trennung zwischen Rechnerraum, Datenträgerarchiv und Arbeitsvor- und -nachbereitung ist sowohl aus Gründen des Datenschutzes als auch der Ordnungsmäßigkeit der Datenverarbeitung bei größeren Rechenzentren zu fordern. Dem muß eine eindeutige Arbeits- und Funktionsteilung im personellen Bereich entsprechen. Ich habe festgestellt, daß diese Funktionstrennung sehr häufig nicht realisiert worden ist.

In einem größeren Rechenzentrum habe ich das völlige Fehlen eines separaten Datenträgerarchivs bemängelt.

Mängel hinsichtlich der Transparenz und der Kontrollierbarkeit der Verfahren

Eine ausreichende Transparenz der Verfahren und die Einhaltung strikter und formeller Vorgehensweisen bei der Freigabe von Verfahren und Programmen sind Voraussetzungen sowohl für die langfristig gesicherte Einsatzfähigkeit eines Verfahrens als auch für die Kontrolle der Verfahren durch die anwendende Stelle oder durch Kontrollinstanzen wie Rechnungshof und Datenschutzbeauftragter.

In einem Falle habe ich festgestellt, daß die geprüfte Stelle nicht verhindert hatte, daß die Zusammenarbeit mit einem privaten Software-Unternehmen zu einer bedenklichen Abhängigkeit von diesem Unternehmen führte. Eine Dokumentation der Verfahren und Programme war nur fragmentarisch vorhanden, die Freigabe erfolgte höchst informell ohne DV-fachlichen Hintergrund bei der freigebenden Stelle. Die sensitiven personenbezogenen Daten waren darüberhinaus in keiner Weise vor Einsichtnahme durch die Fremdfirma geschützt.

Die Dokumentation war auch bei anderen geprüften Stellen nicht vollständig oder nicht systematisch zusammengestellt. Die dabei von mir angelegten Maßstäbe entsprechen den Mindestanforderungen der Rechnungshöfe.

Mängel bei der Durchführung von Programmtests

Bereits die Forderung nach ordnungsgemäßer Datenverarbeitung gebietet, daß Programmtests nicht mit echten personenbezogenen Daten, sondern mit Daten durchgeführt werden, die keinen Rückschluß auf Personen zulassen. Bei den meisten geprüften Stellen habe ich jedoch festgestellt, daß Programmtests mit echten personenbezogenen Daten durchgeführt werden. Dies ist auch dann unzulässig, wenn zum Testen Kopien von Echt-Datenbeständen oder ältere Dateigenerationen aus der Datensicherung verwendet werden. Wenn so vorgegangen wird, wird gegen die Zulässigkeitsvoraussetzungen des §6 Berliner Datenschutzgesetz sowie das Datengeheimnis gem. §8 Berliner Datenschutzgesetz verstoßen, da die Kenntnisnahme geschützter Daten durch die testenden Instanzen nicht erforderlich ist und da die bei Originaltests verwendeten Testdaten und Testergebnisse zur weiteren Einsicht in der Programmdokumentation abzulegen sind.

Mängel bei der Benutzer- und Zugriffskontrolle

Bei einer Stelle habe ich festgestellt, daß - abgesehen von einer unzureichenden Zugangssicherung - eine technisch unterstützte Benutzer- und Zugriffskontrolle nicht durchgeführt wurde, so daß die Terminals nicht ausreichend vor unbefugter Verwendung geschützt waren und eine unzulässige Benutzung auch nicht nachträglich nachweisbar war. Diesem Mißstand wird durch den Einsatz einer auf dem Markt erhältlichen Datenschutz-Software abgeholfen.

Mängel bei der Transportkontrolle

Beim Transport von elektronischen und papierenen Datenträgern von der Datenerhebung zur Datenerfassung, von der Datenerfassung zur Datenverarbeitung, von der Datenverarbeitung zur Datenverwendung sind die Datenträger vor Risiken einer unbefugten Entfernung oder Kenntnisnahme sowie der Veränderung von Daten zu schützen. Diese sogenannte Transportkontrolle wurde vor allem bei papierenen Datenträgern (Belegen, Listen) in einigen Fällen nicht ausreichend durchgeführt.

So habe ich festgestellt, daß Listen und Belege mit sensiblen Sozialdaten in offenen Mappen im Rahmen der Fachpost an die Sozialbehörden der Bezirksämter versandt wurden, ohne daß in jedem Falle eine ausreichende Sicherheit darüber bestand, ob die Abholer überhaupt zum Transport der Fachpost befugt waren. Aufgrund meiner Bemängelung wird der Transport dieser Listen und Belege nunmehr im Rahmen des Datenträger-Container-Verkehrs des LED abgewickelt.

In einer anderen Stelle wurden Belege und Computer-Listen mit Daten, die der ärztlichen Schweigepflicht unterlagen, im Rahmen eines Hol- und Bringedienstes zwischen den verschiedenen Gebäuden dieser Stelle transportiert, bei dem die sensitiven Unterlagen in offenen Einkaufskörben auf Fahrradgepäckträgern untergebracht waren. Die Unterlagen wurden trotz vorhandenen Besucherverkehrs auch dann nicht gesichert, wenn die Fahrräder abgestellt wurden. Die Auslieferung der Unterlagen erfolgte in einem der Gebäude durch Einwerfen in offene Postfächer, die sich im allgemein zugänglichen Foyer befanden. Ich habe aufgrund meiner Bemängelung die Zusage erhalten, daß die ohnehin beabsichtigte Umorganisation des Postverkehrs innerhalb der geprüften Stelle unverzüglich stattfinden würde und die Mängel dadurch beseitigt werden würden.

Formelle Mängel

Ich habe in vielen Fällen nach §22 Berliner Datenschutzgesetz meldepflichtige Dateien aufgefunden, die noch nicht zum Dateienregister gemeldet worden waren.

Darüber hinaus ist die nach §16 Satz 2 Nr. 1 Berliner Datenschutzgesetz vorgeschriebene Übersicht über die Art der gespeicherten personenbezogenen Daten, der Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie deren regelmäßige Empfänger in den meisten Fällen nicht oder nicht korrekt geführt worden.

4. Nachtrag zu Feststellungen aus den Vorjahren 1979 bis 1981

Im Interesse einer besseren Übersichtlichkeit habe ich neue Entwicklungen zu Feststellungen aus den Vorjahren im folgenden Abschnitt zusammengefaßt. Die Zahl der Punkte, bei denen inzwischen eingetretene Verbesserungen des Datenschutzes nachzutragen sind, ist erfreulich. Sie sind ein Zeichen für die Kooperationsbereitschaft der betreffenden Verwaltungen. Darüber dürfen allerdings Defizite bei der Aufarbeitung alter Punkte nicht vergessen werden, von denen ich im folgenden ebenfalls auf die wichtigsten hingewiesen habe mit der Absicht, auch in diesen Bereichen Fortschritte zu erzielen.

4.1 Verbesserungen und Ergänzungen

Forschungsprojekt des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg (Jahresbericht 1981, S. 15)

Im letzten Jahresbericht habe ich darüber berichtet, daß sich Strafgefangene der Justizvollzugsanstalt Tegel an mich gewandt und geltend gemacht hatten, die Persönlichkeitsrechte der Strafgefangenen würden wegen der Art der Durchführung des Forschungsprojektes verletzt. Insbesondere hatten sie sich über die Übermittlung von Daten aus den Gefangenenpersonalakten nach Freiburg beschwert.

Inzwischen ist ein Modell zur Anonymisierung der für die Forschung benötigten Daten entwickelt worden, das sowohl den schutzwürdigen Belangen der Gefangenen als auch dem Forschungsbedürfnis des Max-Planck-Instituts und des Landes Berlin Rechnung tragen kann. Es wurde sichergestellt, daß personenbezogene Daten ohne Einwilligung der Betroffenen nicht mehr an das Max-Planck-Institut nach Freiburg abgegeben werden.

Schließlich hat die für das Max-Planck-Institut zuständige Aufsichtsbehörde, das Innenministerium Baden-Württemberg, eine Überprüfung vor Ort vorgenommen. Aus dem mir mitgeteilten Ergebnis geht hervor, daß nach Durchführung der Verbesserungsmaßnahmen personenbezogene Daten nicht mehr gespeichert werden bzw. alte Daten gelöscht worden sind. Die Angelegenheit erscheint daher durch die konstruktive Mitarbeit aller Beteiligten erledigt.

Gewerberegister (Jahresbericht 1981, S. 16)

In meinem letzten Jahresbericht habe ich auch auf zahlreiche Beschwerden von Gläubigern hingewiesen, die zur Durchsetzung ihrer Forderungen präzise Angaben über ihre Schuldner benötigen, diese aber wegen der bestehenden Rechtslage nicht immer erhalten können. Nach § 11 Berliner Datenschutzgesetz ist die Übermittlung personenbezogener Daten durch die Gewerbeaufsichtsämter an die Gläubiger als nicht-öffentliche Stellen an die Einwilligung der Betroffenen gebunden. Inzwischen sind Vorbereitungen getroffen, die Schwierigkeiten durch eine bundesweite Regelung in der Gewerbeordnung auszuräumen. Dabei ist folgende Regelung vorgesehen:

> § 14 GewO (Anzeigepflicht)
>
> (5) Die Übermittlung personenbezogener Daten aus den Gewerbeanzeigen an Behörden und sonstige öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Die Übermittlung personenbezogener Daten aus den Gewerbeanzeigen an Personen und Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Es steht also zu hoffen, daß die aufgetretenen Schwierigkeiten durch eine entsprechende Regelung beseitigt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat insoweit keine Einwände erhoben als damit die Rechtslage an das Bundesdatenschutzgesetz angeglichen wird.

Ablichtung von Personalausweisen (Jahresbericht 1981, S. 9, Jahresbericht 1980, S. 14)

Bei der Diskussion war noch die Frage offen geblieben, wie das Verfahren der Notare zu beurteilen ist, Fotokopien von Personalausweisen zu fertigen und längere Zeit aufzubewahren.

Nach § 10 Beurkundungsgesetz hat sich der Notar über die Person des an einem Beurkundungsvorgang Beteiligten „Gewißheit" zu verschaffen. Dabei hat der Notar ein Ermessen, auf welche Weise er dabei vorgeht. Allerdings ist im Hinblick auf die förmliche Beweiskraft der notariellen Urkunde (§ 415 ZPO) ein hohes Maß an Sorgfalt aufzuwenden. Der Geschäftsverkehr muß sich darauf verlassen können, daß die beurkundeten Erklärungen oder die beglaubigte Unterschrift wirklich von der Person abgegeben ist, die in der Urkunde als Erklärende oder Urheber der Unterschrift bezeichnet ist.

Vorschriften, welche Beweismittel beizuziehen sind, existieren nicht. Insbesondere gibt es keine Vorschrift, die die Beiziehung zusätzlicher Identifikationsmittel (z.B. Fotokopien) untersagt. Ungeachtet des Umstandes, daß die Kopien zu den Akten genommen werden und damit das Berliner Datenschutzgesetz keine Anwendung findet, ergibt auch die Anwendung der den Datenschutzgesetzen zugrundegelegten Rechtsgedanken nichts anderes: Die Verarbeitung personenbezogener Daten ist danach zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Bei der Beurkundung von Verträgen kann auch im Nachhinein eine Identifikation der Beteiligten erforderlich sein; diese „Spätidentifikation" wird durch das Vorhalten von Kopien in den Beiakten erheblich erleichtert.

Mit der Notarkammer komme ich daher zu dem Ergebnis, daß gegen das in Frage stehende Verfahren datenschutzrechtliche Bedenken nicht bestehen.

Meldewesen (Jahresbericht 1981, S. 8)

Anläßlich der Wahl am 10. Mai 1981 hatte ich 50 Fälle festgestellt, in denen Bürgern Wahlunterlagen zugesandt wurden, obwohl sie wegen geistiger Gebrechen unter Pflegschaft standen oder in denen sie keine Wahlunterlagen erhielten, weil in der Datenbank irrtümlich Wahlausschlußgründe vermerkt waren. Der Senator für Justiz hat mir inzwischen mitgeteilt, daß sein Vorschlag, den Belegfluß zwischen Amtsgericht und Bezirksämtern mit Hilfe eines Empfangsbekenntnisses zu verbessern, verwirklicht sei. Die Projektgruppe Einwohnerwesen beim Senator für Inneres hat zugesagt, der im Zuge der Umsetzung des neuen Melderechts erforderlichen Programmänderungsmaßnahmen das für die Änderungen der Pflegschaftsdaten zu verwendende Aufrufprogramm zusätzlich gegen unbefugte bzw. fehlerhafte Zugriffe zu sichern.

Spätestens bei den nächsten Wahlen wird sich zeigen, ob die getroffenen Maßnahmen ausreichen.

Vergabe der Begleituntersuchung Bildschirmtext (Jahresbericht 1981, S. 14)

In meinem Jahresbericht hatte ich an den Auftrag des Gesetzgebers erinnert, eine Begleituntersuchung durchzuführen (§ 2 Bildschirmtexterprobungsgesetz). Inzwischen ist diese Untersuchung vergeben worden.

Vordrucke zur Beantragung der Sozialhilfe (Jahresbericht 1980, S. 14, Jahresbericht 1979, S. 4)

Bereits 1979 hatte ich die Bedenken hervorgehoben, die gegen die in den bisher verwendeten Vordrucken vorgesehene pauschalierte Einwilligung zur Akteneinsicht bei einer Vielzahl von Stellen bestehen. Inzwischen ist der Vordruck so geändert worden, daß meine Bedenken entfallen.

Aufzeichnung von Ferngesprächen (Jahresbericht 1981, S. 17)

Gegen die automatische Erfassung der angewählten Rufnummern bei Privatgesprächen durch öffentliche Stellen habe ich Bedenken geäußert und empfohlen, die technischen Voraussetzungen dafür zu schaffen, daß die ordnungsgemäße Abrechnung auch ohne Speicherung der Zielnummer sichergestellt werden kann. Eine zwischenzeitlich bei allen Berliner Hochschulen durchgeführte Überprüfung hat ergeben, daß in diesem Bereich kein Verfahren mehr besteht, das zu Bedenken Anlaß gibt. Im Zuge der routinemäßigen Überprüfung werde ich auch bei anderen öffentlichen Stellen dem Problem der automatischen Telefonnummernerfassung nachgehen.

4.2 Defizite

Schülerdaten (Jahresbericht 1981, S. 11f, Jahresbericht 1980, S. 13)

Gegenüber dem Senator für Schulwesen, Jugend und Sport habe ich Ende 1980 eine ausführliche Stellungnahme zu Problemen abgegeben, die sich aus der Führung von Schülerdaten, insbesondere in den Schülerbogen ergeben. Die geplanten Ausfüh-

rungsvorschriften für den Umgang mit Schülerdaten stehen noch aus.

Unbeschränkte Auskünfte aus dem Bundeszentralregister (Jahresbericht 1981, S. 10, Jahresbericht 1980, S. 12)

Meine Feststellungen haben ergeben, daß Berliner Behörden bei verschiedenen Verwaltungsvorgängen (z.B. bei Einstellungen in den öffentlichen Dienst, aber z.B. auch bei der Feststellung der Eignung als Kleinsiedler auf einer Erbbauheimstätte) teilweise in unverhältnismäßigem Ausmaß von der Möglichkeit Gebrauch machen, eine unbeschränkte Auskunft aus dem Bundeszentralregister einzuholen. Eine Regelung des Fragenkomplexes durch den Senat ist angekündigt, aber noch nicht erfolgt.

Umgang mit psychiatrischen Daten (Jahresbericht 1981, S. 7 und S. 20)

Um den Datenschutz in diesem kritischen Bereich zu fördern, habe ich Kriterien für die datenschutzrechtliche Beurteilung der Erhebung, Speicherung und Übermittlung psychiatrischer Daten zusammengestellt, die für Verwaltungszwecke von Dienststellen des Landes Berlin benötigt werden. Eine Stellungnahme zu diesem Vorschlag steht noch aus.

Verordnung über Führung, Inhalt und Aufbewahrung von Krankengeschichten in Krankenhäusern - Krankengeschichtenverordnung (Jahresbericht 1981, S. 6)

Aufgrund der von mir festgestellten erheblichen Mängel in diesem Bereich ist von Seiten des Senats eine baldige Regelung in Aussicht gestellt worden. Diese steht jedoch noch aus.

5. Zusammenarbeit mit anderen Stellen

5.1 Datenschutzbeauftragte des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in drei Sitzungen in Stuttgart unter dem Vorsitz der Landesbeauftragten für den Datenschutz Baden-Württemberg beraten.

Die wichtigsten Ergebnisse lassen sich wie folgt zusammenfassen:

11. Konferenz am 27. April 1982

- Für den Fall, daß die Gesundheitsministerkonferenz einen Musterentwurf eines Krebsregistergesetzes beschließt, hat die Konferenz der Datenschutzbeauftragten Empfehlungen zum vom Bundesminister für Jugend, Familie und Gesundheit vorgelegten Entwurf eines Gesetzes über ein Krebsregister (Stand: Januar 1982) verabschiedet.
- Entschließung zur Begleitforschung und Datenschutz im „Modellprogramm Psychiatrie der Bundesregierung". Die Konferenz beabsichtigt, auf der Grundlage dieser Entschließung eine Abstimmung mit den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich herbeizuführen. Sie ist der Auffassung, daß im Interesse der Forschung wie der Betroffenen eine einheitliche Datenschutzpraxis im privaten und öffentlichen Bereich angestrebt werden sollte.
- Empfehlungen zur Sicherstellung des Datenschutzes im Archivwesen.

12. Konferenz am 21. Juni 1982

- Beschluß einer Stellungnahme zum Referentenentwurf des Bundesministers des Innern zur Änderung des Bundesdatenschutzgesetzes.
- Beschluß über datenschutzrechtliche Regelungen im Staatsvertrag über Bildschirmtext.

13. Konferenz am 28. September 1982

- Beschluß über die Behandlung von Daten über die Befreiung von der Rundfunkgebührenpflicht und die Informationshilfe öffentlicher Stellen für Rundfunkanstalten.
- Beschluß über Fragen des Datenschutzes in der Steuerverwaltung.
- Beschluß über Auskunft aus Gewerbeanzeigen.
- Beschluß über die datenschutzrechtliche Einordnung der Informationszentrale für den Steuerfahndungsdienst beim Finanzamt Wiesbaden II.

Der Vorsitz wird mit dem Jahreswechsel turnusgemäß auf den Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen übergehen.

5.2 Aufsichtsbehörde für nicht-öffentliche Stellen, andere Kontrollbehörden

In den turnusmäßigen Sitzungen mit dem Senator für Inneres als Aufsichtsbehörde für den Datenschutz wurden zahlreiche Grundsatz- und Einzelfragen behandelt. U. a. der Referentenentwurf des Bundesministers des Innern zur Novellierung des Bundesdatenschutzgesetzes, die Geltung des §2 Abs. 3 Berliner Datenschutzgesetz auch bei Schachtelbeteiligungen - z.B. bei der Wohnungsbau-Rechenzentrum GmbH - und das einheitliche Vorgehen im Rahmen des Modellprogramms Psychiatrie unabhängig davon, ob die betroffenen Stellen öffentlich-rechtlich oder privat organisiert sind sowie die Erhebung und Weitergabe von Personaldaten in Zusammenhang mit Bewerbungsvorgängen.

Die Kontaktgespräche mit Datenschutzbeauftragten der Religionsgemeinschaften habe ich in diesem Jahr fortgeführt.

5.3 Berliner Verwaltung

Dateienregister

Bis zum 1. November 1982 sind mir zum allgemeinen und besonderen Dateienregister gemäß §22 Berliner Datenschutzgesetz 79 weitere Dateien gemeldet worden, so daß sich der momentane Stand auf insgesamt 474 Dateimeldungen beläuft. Zum allgemeinen Register wurden 312 Dateien gemeldet, zum besonderen Register gingen 162 Meldungen ein.

Nach meinen Schätzungen dürften von einigen speichernden Stellen, wie z.B. Schulen und Krankenhäusern, trotz mehrfacher Hinweise noch nicht alle Dateien gemeldet sein. Ich habe daher Anfang Mai 1982 eine Nachfaßaktion gestartet, mit dem Ziel, sämtliche öffentliche Stellen Berlins zu erreichen, die noch nicht zu einem der beiden Register gemeldet haben.

Beim Vergleich der Meldungen zum Amtsblatt für Berlin und zum Dateienregister mußte ich mehrfach feststellen, daß die Angaben über die Adressaten regelmäßiger Übermittlungen erheblich voneinander abwichen.

Auf Datenträgern, die für den Einsatz auf den zunehmend eingesetzten Textautomaten eingesetzt werden, werden häufig Dateien mit personenbezogenen Daten geführt. Aus gegebenem Anlaß weise ich darauf hin, daß auch solche Dateien in der durch die Datenschutzregisterordnung vorgesehenen Form zu melden sind.

Mit der Führung des Dateienregisters sind zwei Zielsetzungen verbunden:

Zum einen stellt es ein wichtiges Hilfsmittel bei der Überprüfung von Rechenzentren und Rechenstellen dar. Die in Berlin vorgesehene relativ detaillierte Form der Meldung, insbesondere auch in Bezug auf die eingesetzten Datenverarbeitungsanlagen, kommt dieser Zielsetzung sehr entgegen.

Zum anderen soll das Dateienregister aber auch gegenüber dem Bürger größtmögliche Transparenz der Datenverarbeitung im öffentlichen Bereich herstellen. Zwar kann der Bürger dem Register nicht, wie oft irrtümlich angenommen, entnehmen, welche Daten konkret von ihm in der Berliner Verwaltung gespeichert sind. Aufgrund seiner Kontakte mit der Verwaltung kann er jedoch einschätzen, welche Stellen personenbezogene Daten von ihm speichern könnten.

Gleichwohl wird von der Möglichkeit der Einsichtnahme in das (allgemeine) Dateienregister relativ wenig Gebrauch gemacht. Dies liegt sicherlich auch daran, daß die Sammlung der Registermeldungen alleine dem Bürger die erforderliche Übersicht nicht verschafft.

Aus diesem Grunde habe ich mit einem mir zur Verfügung stehenden Textautomaten die Registermeldungen in gestraffter Form nochmals erfaßt und mit Hilfe eines Stichwortverzeichnisses zugänglich gemacht. Der interessierte Bürger kann daraus ersehen, zu welchen betroffenen Personenkreisen er gehört und gegebenenfalls einen Ausdruck des Kurzeintrags anfordern bzw. in der Dienststelle einsehen.

Änderung der gemeinsamen Geschäftsordnung für die Berliner Verwaltung, allgemeiner Teil (GGO I)

Einige Schwierigkeiten bei der Durchsetzung des Datenschutzgedankens im Geschäftsverkehr beruhen darauf, daß die geltende gemeinsame Geschäftsordnung für die Berliner Verwaltung datenschutzrechtliche Bestimmungen noch nicht enthalten konnte. Anläßlich der vom Senator für Inneres beabsichtigten Überarbeitung der GGO I habe ich zahlreiche Vorschläge unterbreitet, die den Mitarbeitern der Berliner Verwaltung ein einheitliches, datenschutzgerechtes Vorgehen erleichtern soll. Meine Vorschläge betreffen zum einen die Einbeziehung des Berliner Datenschutzbeauftragten bzw. behördlicher Datenschutzbeauftragten im Geschäftsgang sowie die Berücksichtigung materieller Kriterien für den Umgang mit schutzwürdigen Daten.

Wertvolle Anregungen bietet der als Anlage 2 beigefügte Entwurf für eine Verfahrensvorschrift zur Datensicherung bei manuellen Datensammlungen, der von Studierenden des Fachstudiums aus dem Studiengang 20/1979 der Verwaltungsakademie Berlin erstellt worden ist.

Eine entsprechende Änderung der GGO I könnte bewirken, daß im einfachen Geschäftsverkehr der Datenschutzgedanke von vornherein berücksichtigt wird. Dies wäre für die Verwaltungsmitarbeiter eine wesentliche Hilfe.

6. Aufgaben des Berliner Datenschutzbeauftragten

6.1 Im Berichtsjahr 1982

Anrufungen durch jedermann

Die Zahl der Eingaben hat gegenüber dem Vorjahr um ca. 50% zugenommen. Die Anrufungen erstrecken sich nach der Häufigkeit geordnet insbesondere auf folgende Gebiete:

1. Öffentliche Sicherheit und Ordnung
2. Sozial- und Gesundheitswesen
3. Wirtschaftsverwaltung
4. Finanz- und Steuerwesen
5. Bau- und Wohnungswesen.

In ca. 50% aller Eingaben haben sich Mängel herausgestellt. Bemerkenswert ist, daß der Prozentsatz der Mängel im Bereich öffentliche Sicherheit und Ordnung geringer ist (ca. 30%).

Den Bund, die Kirchen und den Bereich der Privatwirtschaft betreffende Eingaben habe ich an die zuständigen Stellen abgegeben.

An mich sind auch zahlreiche Beschwerden über die unverlangte Zusendung von Werbematerialien herangetragen worden. Soweit sie den privaten Bereich betreffen, ist hierfür der Senator für Inneres – I D – als Aufsichtsbehörde zuständig, sofern das betreffende Unternehmen seinen Sitz in Berlin hat.

Beratung und Kontrolle

Die Anzahl der Beratungsersuchen (§ 21 Abs. 1 letzter Satz Berliner Datenschutzgesetz) hat erneut zugenommen. Zu den Schwerpunkten gehörten:

- Das Bau- und Wohnungswesen
- die Neuen Medien
- der Bereich öffentliche Sicherheit und Ordnung.

Öffentlichkeitsarbeit

In der Aufbauphase ist es gelungen, gute Kontakte zur Bevölkerung und zu den Medien herzustellen. Es ist immer wieder erstaunlich festzustellen, in welchem Umfange auch Anfragen aus dem übrigen Bundesgebiet und sogar aus dem Ausland eintreffen. Dazu haben Veröffentlichungen zu den Neuen Medien, die auch im Ausland auf besonderes Interesse gestoßen sind, das Datenscheckheft und die Broschüre „Gesetze zum Datenschutz" beigetragen, die in diesem Jahr neu aufgelegt worden ist.

In Berlin habe ich mich mit meinen Mitarbeitern vor allem bemüht, durch Vortragsveranstaltungen das Interesse am Datenschutz zu verstärken. So wurde zusammen mit Herrn Professor Dr. Jarass im Sommersemester 1982 ein Seminar an der Freien Universität abgehalten mit dem Thema „Aktuelle Probleme des Datenschutzes in Wirtschaft und Verwaltung". An der Richterakademie in Trier habe ich zusammen mit einem Vertreter des bayerischen Landesbeauftragten Datenschutzprobleme dargestellt. Ferner wurden Veranstaltungen an der Verwaltungsakademie und der Fachhochschule für Sozialarbeit und Sozialpädagogik durchgeführt. Schließlich waren auch zahlreiche Besucher aus dem In- und Ausland zu verzeichnen, die sich insbesondere über Datenschutzfragen bei den Neuen Medien informiert haben.

Aufbau der Dienststelle

Die im Jahresbericht 1981 geschilderte personelle Situation[18] hat sich angesichts des Anstiegs der Eingaben und der Beratungsvorgänge weiter angespannt.

Es war daher unumgänglich, die bereits für die Vorjahre vorgesehene personelle Verstärkung zu beantragen. Die Unterstützung meiner entsprechenden Anträge durch alle im Parlament vertretenen Fraktionen ermöglicht mir nicht nur die kontinuierliche Fortsetzung meiner Arbeit, sondern zeigt zugleich das besondere Interesse der Parlamentarier am Datenschutz.

6.2 Voraussichtliche Schwerpunkte der künftigen Arbeit

Aufgrund der bisherigen Erfahrungen ergeben sich folgende Schwerpunkte für das Jahr 1983:

a) Erledigung der Anliegen, die die Bürger mit ihren Eingaben verfolgen.

   Trotz der stark gestiegenen Zahl von Eingaben, sehe ich es als meine Hauptaufgabe an, diese möglichst zügig zu erledigen.

b) Überprüfungen von Amts wegen und Beratungen
   - Neue Medien (Bildschirmtexterprobung, Kabelfernsehprojekt, Gesetzgebung zur Medienerprobung)
   - Kulturelle Einrichtungen
   - Öffentliche Sicherheit und Strafverfolgung
   - Datensammlungen in der Psychiatrie
   - Datenverarbeitung bei Eigenbetrieben
   - Datenverarbeitung im Klinikum Steglitz der Freien Universität.

Gegenstand der Überprüfungen sind sowohl die datenschutzrechtlichen Voraussetzungen als auch die Maßnahmen zum organisatorischen und technischen Datenschutz.

6.3 Absehbare Entwicklungen

Novellierung des Bundesdatenschutzgesetzes

Die für diese Legislaturperiode geplante Novellierung des Bundesdatenschutzgesetzes hat mit der Vorlage des Referentenentwurfs vom 31. März 1982 Gestalt angenommen. Danach sind folgende Änderungen beabsichtigt:

- Der Entwurf bezieht die Datenerhebung mit ein, so daß der Begriff „Datenverarbeitung" entsprechend erweitert wird,
- ferner ist ein verschuldensunabhängiger Schadensersatzanspruch ohne Obergrenze vorgesehen.
- Die Auskunft für den Bürger soll in Zukunft im wesentlichen unentgeltlich sein.

[18] S. 4

- Der zunehmenden Bedeutung der Datenfernverarbeitung wird durch neue Regelungen für sog. On-line-Übermittlungen Rechnung getragen.
- Die Auskunftspflicht soll auf die Quelle und Empfänger der Daten erweitert werden.
- Bei Datenübermittlungen soll der Grundsatz der Zweckbindung stärker gelten.
- Der Datenschutz bei den Medien (Rundfunkanstalten des Bundes) soll verbessert werden.
- Für den betrieblichen Datenschutzbeauftragten ist ein besonderer Kündigungsschutz vorgesehen.
- Die Stellung des Bundesbeauftragten für den Datenschutz soll gestärkt werden.
- Die Kompetenzen der Aufsichtsbehörden sollen erweitert werden.
- Die Amtshilfe wird näher geregelt.

Der Referentenentwurf sieht damit praktische Verbesserungen des Datenschutzes für den Bürger vor, ohne daß die - bewährte - Konzeption und Systematik des Gesetzes geändert wird.

Die vorgeschlagenen Änderungen wären zum Teil auch für das Berliner Datenschutzgesetz relevant. Da das Berliner Datenschutzgesetz zu den neueren Datenschutzgesetzen zählt und daher auch einige Regelungen enthält, die in das Bundesdatenschutzgesetz erst eingefügt werden sollen, vertrete ich nach wie vor die Meinung, daß die Ergebnisse auf Bundesebene abgewartet werden können, bevor eine Änderung des Berliner Datenschutzgesetzes erfolgt. Die vorgesehenen Neuwahlen des Bundestages geben Gelegenheit, das Novellierungsvorhaben noch einmal kritisch daraufhin zu überdenken, ob das Gewicht der Vorschläge eine sofortige Neuregelung erforderlich macht.

Entwurf einer Verwaltungsprozeßordnung

Daß auch andere Gesetzesvorhaben datenschutzrelevant sind, zeigt der von den Bundesministerien für Justiz sowie für Arbeit und Sozialordnung vorgelegte Entwurf einer Verwaltungsprozeßordnung. Ich habe gegenüber dem Senator für Justiz u.a. auf folgende Verbesserungsmöglichkeiten hingewiesen:

Der Ausschluß der Öffentlichkeit soll nach wie vor in § 172 Gerichtsverfassungsgesetz seine Grundlage finden; danach *kann* die Öffentlichkeit ausgeschlossen werden, wenn eine Verletzung überwiegender schutzwürdiger Interessen bei Umständen aus dem persönlichen Lebensbereich oder wichtigen Geschäfts-, Betriebs-, Erfindungs- oder Steuergeheimnissen droht. Durch eine neue Bestimmung (§ 47 des Entwurfs) soll nunmehr das Gericht bei einem entsprechenden Antrag *verpflichtet* werden, die Öffentlichkeit dann auszuschließen, wenn Tatsachen erörtert werden, die dem Steuergeheimnis oder dem Sozialgeheimnis [illegible]. Zu prüfen wäre hier, ob diese Vorschrift nicht auf andere besondere Berufs- und Amtsgeheimnisse auszudehnen wäre (z.B. Statistikgeheimnis, ärztliche Schweigepflicht).

Mit der Möglichkeit des Ausschlusses der Öffentlichkeit ist nicht das Problem gelöst, daß auch bei einer Erörterung entsprechender Angelegenheiten in nicht-öffentlicher Verhandlung jedenfalls allen Prozeßbeteiligten die erörterten Umstände offenbart werden. Für den Fall, daß sich herausstellt, daß die erörterten Tatsachen nicht entscheidungsrelevant sind, steht der Beeinträchtigung der Privatsphäre kein hinreichender prozessualer Zweck gegenüber. Es wäre erwägenswert, hier prozessual ein Zwischenverfahren vorzusehen, in dem auskunftspflichtige Prozeßbeteiligte oder Dritte zunächst nur dem Gericht die personenbezogenen Daten offenbaren. Das Gericht entscheidet dann darüber, ob diese Daten in den Prozeß eingeführt werden sollen oder nicht. Ein solches „in-camera-Verfahren" ist im anglo-amerikanischen Recht bekannt[1].

Ein ähnliches Problem stellt sich bei der Frage, in welchem Umfang Prozeßbeteiligte oder Dritte zur Herausgabe von Daten verpflichtet sein sollen. Gegenüber der derzeitigen Rechtslage - die von dem mißverständlichen Begriff der „ihrem Wesen nach geheimzuhaltenden" Vorgänge ausgeht - sieht der Entwurf vor, daß eine Verpflichtung zur Vorlage von Unterlagen und zur Auskunft nicht besteht, wenn diese unter Berücksichtigung aller Umstände unzumutbar ist: Unklar bleibt, auf wen die Zumutbarkeit zu beziehen ist. Auf den Vorlage- bzw. Auskunftspflichtigen oder auf den (von der Information) Betroffenen. Das von Seiten des (privaten) Auskunftspflichtigen einschlägige Bundesdatenschutzgesetz stellt hier auf die schutzwürdigen Belange des Betroffenen ab (§ 24). Die Vorschrift sollte deutlich zum Ausdruck bringen, ob und auf welche Weise die schutzwürdigen Belange einzubringen sind bzw. inwieweit die Bestimmungen des Bundesdatenschutzgesetzes verdrängt werden. Auch hier wäre bei Zweifelsfällen die Eröffnung eines in-camera-Verfahrens denkbar.

Berlin, den 28. Dezember 1982

Der Berliner Datenschutzbeauftragte

Dr. Kerkau

[1] Vgl. z. B. Zift 4 B U.S. Freedom of information act

Anlage 1

Vorstellungen über datenschutzrechtliche Anforderungen an Gesetze auf dem Gebiet der Neuen Medien, insbesondere Bildschirmtext

(Stand März 1982)

I. Voraussetzungen

1. Der Datenschutz ist abhängig von den Eigenarten der eingesetzten technischen Einrichtungen. Angesichts der zunehmenden Integration einzelner Technologien (Fernsprechen, Fernschreiben, Fernsehen, Datenverarbeitung usw.) sind die Einrichtungen entsprechend ihrer **Funktion** beim Kommunikationsprozeß zu **unterscheiden.**

   Den isolierten Betrieb einzelner Informationsmedien ersetzen die Neuen Medien durch einen Verbund, der die (tendenziell beliebige) Verknüpfung der „klassischen Medien" gestattet (z.B. Btx: Telefon - Fernsehen - Datenverarbeitung). Der bisher isoliert entsprechend den beteiligten Medien betrachtete Datenschutz (Fernmeldegeheimnis, Medienrecht mit den entsprechenden Medienprivilegien, Datenschutzgesetze, im formellen Sinn) muß nun bezogen werden auf die verschiedenen, am Verbund beteiligten Funktionsebenen:

   - Ebene des Informationstransports (technische Übertragung)
   - Ebene der Informationsbereithaltung
   - Ebene der Informationsanwendung durch die Teilnehmer.

   Jede dieser Ebenen bedarf einer eigenständigen Betrachtung.

2. Die Regelung des Datenschutzes fällt in die **Zuständigkeit** derjenigen Stellen, denen Regelungskompetenz im Hinblick auf die einzelnen Einrichtungen zukommt (Annexprinzip).

   Die - verfassungsrechtlich festgeschriebenen - Gesetzgebungskompetenzen knüpfen demgegenüber an der bisherigen technologischen Situation an:

   - Fernsprechnetz, Fernschreibnetz, Datenübertragungsnetz: Bund
   - Fernsehen, Presse, Rundfunk („Massenmedien"): Land (ggf. Rahmenkompetenz)
   - Benutzung der Medien zur Erfüllung eigener Zwecksetzungen: Bund (Bundesbehörden, Private) und Land (Landesbehörden).

   Der Einsatz Neuer Medien erfordert eine Projektion dieser Zuständigkeiten auf die jeweiligen Funktionsebenen. Daraus ergibt sich:

   - Transportfunktion: Bundeskompetenz
   - Bereithaltungsfunktion: Landeskompetenz
   - Anwendungsfunktionen: gemischte Kompetenz; ggf. Landeskompetenz im Hinblick auf zulässige Nutzungen der Bereitstellungseinrichtungen.

3. Bezugspunkt für den Datenschutz ist die Verantwortlichkeit der speichernden Stelle. Dies setzt eine eindeutige Regelung der **Trägerschaft** der beteiligten Einrichtungen voraus.

   Die Trägerschaft ist abhängig von der Regelungskompetenz: Da das Gesamtsystem der Neuen Medien aus Elementen besteht, für die unterschiedliche Kompetenzen gelten, ist auch eine unterschiedliche Trägerschaft zu fordern.

   Hier bieten sich an:

   - für den Transportbereich: Bundespost
   - für den Bereitstellungsbereich: Landesanstalt, -körperschaft; ggf. Privatunternehmen unter Landesaufsicht (vgl. Bayer. Kabelmodell)
   - für den Anwendungsbereich: Trägerschaften sind vorgegeben.

4. Dem Datenschutz unterfallen alle personenbezogenen Daten, die beim Betrieb anfallen, unabhängig von der Art der Speicherung (vgl. Grds. 1.3)[1]. Sie lassen sich einteilen in die Daten, die zum Abruf bereitgehalten werden **(Angebotsdaten)**, und in die Daten, die während der Teilnehmeraktivitäten (Einspeicherung und Abruf) durch Protokollierung der Aktivitäten entstehen **(Teilnehmerdaten).**

   Zweck jeder (auch technischer) Kommunikation ist der Erwerb von Informationen, die für das eigene Verhalten von Bedeutung sind. Die Neuen Medien stellen solche Informationen zur Verfügung bzw. vermitteln den Zugriff auf solche Informationen. Die Teilnehmer haben die Möglichkeit, diese Informationen einzuspeichern (Anbieter) und nach vorgegebenen Kriterien (Suchbaum) abzurufen (Angebotsdaten).

   Jede Aktivität eines Teilnehmers kann protokolliert werden (Teilnehmerdaten). Der Umfang kann verschieden sein. Er reicht von der Aufzeichnung der Tatsache der Nutzung des Systems über die Registrierung des Aufrufs bestimmter Angebote bis hin zur totalen Speicherung der abgerufenen oder eingegebenen Information.

5. Der Datenschutz kann nicht die Verarbeitung personenbezoner Daten generell regeln; es ist vielmehr zwischen den verschiedenen Phasen der Verarbeitung zu unterscheiden.

   Die Datenschutzgesetze unterscheiden folgende Formen der Verarbeitung personenbezogener Daten:

   - Erhebung der Daten (in On-line-Systemen: Abruf von Daten), d. h. die zunächst noch nicht auf dauernde Verwertung oder Auswertung bezogene Beschaffung und Fixierung von Daten
   - Speicherung von Daten, d.h. die (in der Regel geordnete) Erfassung von Daten auf einem Datenträger zum Zweck der weiteren Verwendung
   - Offenbarung von Daten, d. h. die Bekanntgabe von Daten an Stellen, die am Kommunikationsprozeß nicht beteiligt sind (bzw. waren); ein Sonderfall ist die Übermittlung von Daten, d. h. die Bekanntgabe der Daten an dritte Stellen (Unterschied: Die Bekanntgabe von Daten an nicht zuständige Mitglieder der speichernden Stelle ist zwar eine Offenbarung, aber keine Übermittlung)
   - Veränderung von Daten, d. h. die inhaltliche Umgestaltung; eine Sonderform ist die Anonymisierung, d. h. die Veränderung derart, daß die Person, auf die sich die Daten beziehen (Betroffener) nicht mehr erkennbar ist
   - Sperrung von Daten, d.h. die Anbringung eines Vermerks, der die Nutzung der Daten nur noch zu bestimmten Zwecken, insbesondere zur Beweissicherung zuläßt. Als Sperrung gilt auch die gesonderte Aufbewahrung, wenn der Eingriff nur noch zu diesen Zwecken möglich ist
   - Löschen von Daten, d.h. das Unkenntlichmachen der Daten.

II. Leitsätze

1. Grundsätze

1. Im Hinblick auf die datenschutzrechtliche Verantwortlichkeit haben die Gesetze die **Trägerschaft** und die **Grenzen der einzelnen Funktionsbereiche** eindeutig festzulegen.

   Einzubeziehen sind:

   - der technische Übertragungsbereich (Transporteinrichtungen, z.B. Telefon, Leitungsnetz)
   - der (Fern-)verarbeitungsbereich, der den Informationsabruf ermöglicht (Bereitstellungseinrichtungen, z.B. Btx-Zentrale, Kabelzentrale)

[1] Hinweis auf die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedeten Grundsätze (veröffentlicht im Jahresbericht 1981 S. 216 ff.).

– der Anwendungsbereich mit den Datenstationen der Teilnehmer (Teilnehmereinrichtungen, z.B. Fernsehapparat, Drucker, externer Rechner).

Besondere Bedeutung kommt den Bereitstellungseinrichtungen zu, die für den Betrieb der Neuen Medien grundlegend sind.

2. Die Träger sind einem besonderen **Datengeheimnis** zu unterwerfen, das die Teilnehmer- und die Angebotsdaten umfaßt (letztere soweit diese nicht für den Abruf durch jedermann geöffnet sind).

3. Die beteiligten Träger sind lückenlos der Datenschutzkontrolle zu unterwerfen.

4. **Alle Phasen** der Verarbeitung personenbezogener Daten (außer der Löschung) sind, ungeachtet der Verarbeitungsform (vgl. Grds. 1.3), nur unter ausdrücklich benannten Voraussetzungen zulässig.

5. Dem **Betroffenen** ist gegenüber jedem Träger ein unbeschränkter Anspruch auf Auskunft über die von ihm gespeicherten Daten, ein Anspruch auf die Berichtigung falscher Daten sowie ein Anspruch auf Löschung der Daten bei rechtswidriger (Teilnehmerdaten) oder seine schutzwürdigen Belange verletzender Speicherung (Angebotsdaten) einzuräumen.

2. **Technischer Übertragungsbereich (Transporteinrichtungen)**

6. Von der Gesetzgebungszuständigkeit des Bundes sowie der Trägerschaft der Bundespost ist auszugehen.

7. Es ist sicherzustellen, daß das Fernmeldegeheimnis auch für die Daten Geltung besitzt, die Bediensteten der Bundespost beim Betrieb offenbart werden. Einschränkungen des Fernmeldegeheimnisses (z.B. G 10) sollten ausgeschlossen werden (vgl. Grds. 6.).

8. Es ist sicherzustellen, daß der Bundesbeauftragte für den Datenschutz die Einhaltung von Datenschutzvorschriften in den Transporteinrichtungen kontrollieren kann; das Fernmeldegeheimnis ist insoweit einzuschränken (vgl. Grds. 7.1).

9. Die Erhebung personenbezogener Daten ist nur zulässig, soweit dies zur Abwicklung der technischen Übertragung erforderlich ist. Zur Gebührenabrechnung sind die Daten in einer Form zu erheben, die die Art der Nutzung sowie die abgerufenen Informationen nicht mehr erkennen läßt (vgl. Grds. 1.5).

10. Die Speicherung personenbezogener Daten ist abgesehen von den zur Gebührenabrechnung erforderlichen Daten unzulässig. Für die Speicherung personenbezogener Daten zur Kontrolle der Richtigkeit von Gebührenforderungen (z.B. Aufschaltung) ist die Einwilligung der Betroffenen einzuholen.

3. **Bereitstellungseinrichtungen**

3.1 Allgemeines

11. Die Bereitstellungseinrichtungen dienen nicht der technischen Übermittlung, sie unterliegen damit weder der Gesetzgebungskompetenz des Bundes noch der gesetzlichen Trägerschaft der Bundespost. Mangels Normierung im GG sind für die Gesetzgebung damit die Länder zuständig.

12. Aus der Sicht des Datenschutzes ist eine gesetzliche Lösung der Trägerschaft vorzuziehen, die eine unter öffentlicher Aufsicht stehende Institution mit der Trägerschaft betraut; sollte diese Institution privatrechtlich organisiert sein, ist die öffentliche Aufsicht ausdrücklich sicherzustellen.

13. Für den Bereitstellungsbereich ist ein dem Fernmeldegeheimnis vergleichbares Amtsgeheimnis zu schaffen (vgl. Grds. 6.2). Für die in den Einrichtungen dieses Bereichs beschäftigten Bediensteten ist ein Zeugnisverweigerungsrecht und für alle dort gespeicherten Daten ein Beschlagnahmeverbot (vgl. § 97 StPO) zu verlangen (vgl. Grds. 6.4).

14. Neben dem Anbieter muß der Träger der Bereitstellungseinrichtung die rechtliche und technische Möglichkeit haben, den datenschutzrechtlichen Vorschriften Geltung zu verschaffen, insbesondere durch Sperrung oder Löschung einzelner Angebotsdaten oder durch den Entzug der Anbietererlaubnis. Zur Überprüfung ist ein geeignetes Verfahren vorzusehen, das auch den Anspruch auf rechtliches Gehör sicherstellt.

15. Die Einrichtungen im Bereitstellungsbereich sollten der Kontrolle des jeweiligen Landesbeauftragten für den Datenschutz unterstellt werden. Das besondere Amtsgeheimnis (vgl. 13.) ist insoweit einzuschränken (vgl. Grds. 7.1). Dies gilt auch, wenn der Träger in privater Rechtsform gegründet wird. Die Kontrollbefugnis erstreckt sich auf alle Daten, die in Bereitstellungseinrichtungen gespeichert oder vermittels der Bereitstellungseinrichtungen (z.B. aus externen Computern) abrufbar sind (vgl. Grds. 7.1).

3.2 Angebotsdaten

16. Die Speicherung personenbezogener Daten im Rahmen des Informationsangebots (Angebotsdaten) ist nur zulässig, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Wird die Speicherung von öffentlichen Stellen vorgenommen, dürfen nur solche personenbezogenen Daten gespeichert werden, deren unbeschränkte Übermittlung an nichtöffentliche Stellen zulässig ist. Personenbezogene Daten, die sich auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen beziehen, dürfen nicht gespeichert werden. Die Speicherung personenbezogener Daten ist zulässig, wenn der Betroffene unter den Voraussetzungen der entsprechenden Bestimmungen der Landesdatenschutzgesetze zugestimmt hat.

17. Die Übermittlung personenbezogener Daten an jedermann ist zulässig, soweit nicht schutzwürdige Belange der Betroffenen die Beschränkung der Übermittlungsmöglichkeit auf bestimmte Teilnehmergruppen erfordern oder der Anbieter eine Beschränkung ausgesprochen hat. In diesem Fall sind hinreichende Maßnahmen der Datensicherung zu treffen, die einen unberechtigten Abruf verhindern.

18. Angebotsdaten sind vom Träger der Bereitstellungseinrichtung zu sperren, wenn sich weder die Richtigkeit noch die Unrichtigkeit der gespeicherten Daten nachweisen läßt oder wenn die Löschung der gespeicherten Daten zu Zwecken der Beweissicherung oder zur Wahrung sonstiger schutzwürdiger Belange der Beteiligten noch erforderlich ist.

19. Angebotsdaten sind zu löschen, wenn ihre Speicherung in einer Bereitstellungseinrichtung unzulässig ist. Sie sind ferner zu löschen, wenn der Betroffene dies verlangt und begründet darlegt, durch die Speicherung in seinen schutzwürdigen Belangen verletzt zu sein.

3.3 Teilnehmerdaten / Betriebsdaten

20. Teilnehmerdaten dürfen nur erhoben, gespeichert oder übermittelt werden, soweit dies für den Betrieb unumgänglich ist und ohne sie eine der gesetzlich zugelassenen Kommunikationsformen der Neuen Medien nicht durchgeführt werden kann (vgl. Grds. 1.2). Soweit Teilnehmerdaten verarbeitet werden können, dürfen sie nur zu dem Zweck verwertet werden, zu dem sie offenbart werden (Grundsatz der Zweckbindung; vgl. Grds. 4.1).

21. Gebühren und Entgelte für den Abruf der Angebotsdaten sind so zu berechnen und abzurechnen, daß die Art der Nutzung sowie die abgerufenen Daten nicht mehr erkennbar sind (vgl. Grds. 1.5).

22. Personenbezogene Daten, die der Teilnehmer an Bereitstellungseinrichtungen (z.B. über den Rückkanal) übermittelt hat, dürfen im Informationsangebot eines anderen Teilnehmers nur gespeichert werden, wenn er vor der Übermittlung über die Speicherung informiert worden ist.

23. Die Erstellung von Teilnehmerprofilen auf Grund von Teilnehmerdaten ist zu verbieten (vgl. Grds. 3.1).

4. Anwendungsbereich: Teilnehmereinrichtungen

24. Die Zulässigkeit der Verarbeitung personenbezogener Daten durch die Teilnehmer, insbesondere die Übermittlung personenbezogener Daten an Bereitstellungseinrichtungen, richtet sich nach den jeweils anwendbaren Datenschutzgesetzen. Im Hinblick auf die Gesetzgebungskompetenz der Länder sollten jedoch im Zusammenhang mit der Regelung des Bereitstellungsbereichs Zugangsbedingungen für die Teilnehmer formuliert werden, die Informationen anbieten wollen. Ferner sollte ein Anbieter nur zugelassen werden, wenn er zuverlässig ist (u. a. keine Verstöße gegen Datenschutzbestimmungen vorliegen).

25. Der Anschluß von Rechnern durch die Teilnehmer (externe Rechner) ist nur unter der Bedingung zulässig, daß die Möglichkeiten der Erhebung, Speicherung und Übermittlung personenbezogener Daten durch diesen Rechner, die unter 3. verzeichneten Voraussetzungen für Bereitstellungseinrichtungen erfüllen. Dies gilt auch für Daten, die aus weiteren angeschlossenen Rechnern abgerufen oder dorthin übermittelt werden sollen. Hinreichende technische und organisatorische Maßnahmen müssen gewährleisten, daß die Daten nicht unbefugt verarbeitet werden können (vgl. Grds. 7.2).

26. Die Erhebung personenbezogener Daten durch Teilnehmer ist nur zuzulassen, wenn der Betroffene seine Einwilligung hierzu erteilt hat. Dies gilt auch für die Erhebung der Daten durch externe Rechner. Die Übermittlung dieser Daten setzt ebenfalls die Einwilligung der Betroffenen voraus. Durch die Absendung einer Mitteilung, durch die einem Anbieter die Begründung eines Rechtsverhältnisses angetragen wird, gilt die Einwilligung als insoweit erteilt, als dies zur Abwicklung desselben erforderlich ist und dabei die schutzwürdigen Belange der Betroffenen hinreichend gewährleistet werden.

27. Abstimmungen, Wahlen und Meinungsumfragen über den Rückkanal sollten ausgeschlossen werden (vgl. Grds. 4.3).

28. Es ist sicherzustellen, daß in Medienarchiven gespeicherte personenbezogene Daten nicht unter Berufung auf das Medienprivileg frei zugänglich gemacht werden. Eine Speicherung solcher Daten in Bereitstellungseinrichtungen sollte nur unter den Bedingungen von 3. zulässig sein (vgl. Grds. 5.).

29. Für die rechtwidrige Speicherung von Teilnehmerdaten sind Strafvorschriften vorzusehen. Die Speicherung personenbezogener Daten im Angebot, die schutzwürdige Belange der Betroffenen verletzen, ist als Ordnungswidrigkeit zu ahnden; wegen mehrfacher Verstöße ist die Möglichkeit vorzusehen, einen Teilnehmer auszuschließen. Der Abruf von Daten bleibt straffrei, wenn die Daten rechtswidrig gespeichert oder nicht hinreichend gesichert sind (vgl. § 41 Abs. 1 Ziff. 2 BDSG).

Anlage 2

Entwurf für eine Verfahrensvorschrift zur Datensicherung bei manuellen Datensammlungen[1]

I. Grundsätze

§ 1

(1) Wer personenbezogene Daten nutzt, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um einen Mißbrauch der Daten, insbesondere die unbefugte Offenbarung zu verhindern.

(2) Dies gilt ungeachtet der Form, in der personenbezogene Daten aufbewahrt oder übermittelt werden. Ausgenommen sind im folgenden Daten, die automatisch verarbeitet werden.

§ 2

Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

II. Definitionen

§ 3

Personenbezogene **Daten** sind alle Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Soweit schutzwürdige Belange über den Tod hinaus fortwirken, sind auch die Daten Verstorbener wie personenbezogene Daten zu behandeln.

§ 4

Personenbezogene **Vorgänge** sind im Zusammenhang stehende Schriftstücke und andere Datenträger, die sich auf eine bestimmte Person beziehen. Hierzu zählen auch Schriftstücke und Datenträger, die sich auf einen bestimmten Sachverhalt beziehen und personenbezogene Daten enthalten.

§ 5

Personenbezogene **Sammlungen** sind Gesamtheiten von personenbezogenen Vorgängen. Personenbezogene Sammlungen sind dann Dateien, wenn sie gleichartig aufgebaut, nach bestimmten Merkmalen erfaßt und geordnet sind und nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden können.

III. Schutzstufen

§ 6

Jede personenbezogene Sammlung unterliegt einer der folgenden Schutzstufen. Die einzelnen in der Sammlung enthaltenen Vorgänge sowie deren personenbezogene Daten unterliegen dieser Schutzstufe, soweit nicht aus besonderen Gründen im Einzelfall eine höhere Schutzstufe erforderlich ist.

§ 7

Schutzstufen sind

(0) offen
(1) geschützt
(2) vertraulich
(3) streng vertraulich

[1] Aus: Datensicherung bei manuellen Datensammlungen, Entwurf einer Verfahrensvorschrift, ein Projektbericht aus dem Fachstudium der Verwaltungsakademie Berlin, Kurfürstendamm 207-208, 1000 Berlin 15. Erstellt von Studierenden des Fachstudiums aus dem Studiengang 20/1979. Herausgeber: Verwaltungsakademie Berlin, Juni 1982

Zu (0):

Offen sind alle Sammlungen, die jedermann zugänglich sind, insbesondere Presseerzeugnisse und öffentliche Verzeichnisse.

Zu (1):

Geschützt sind alle Sammlungen, wenn die unbefugte Nutzung einzelner in ihnen enthaltener personenbezogener Daten höchstens eine Belästigung erwarten läßt.

Zu (2):

Vertraulich sind alle Sammlungen, wenn die unbefugte Offenbarung der in ihnen enthaltenen personenbezogenen Daten eine Gefährdung der wirtschaftlichen oder gesellschaftlichen Stellung des Betroffenen erwarten läßt. Vertraulich sind insbesondere alle Sammlungen, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen.

Zu (3):

Streng vertraulich sind alle Sammlungen, wenn die unbefugte Offenbarung der in ihnen enthaltenen personenbezogenen Daten einen Eingriff in den unantastbaren Bereich privater Lebensgestaltung darstellen oder Leben, Gesundheit oder Freiheit der Betroffenen gefährden würde.

§ 8

Dateien sind mindestens als geschützte Sammlungen zu behandeln.

IV. Zuordnung zur Schutzstufe

§ 9

Die Zuordnung personenbezogener Sammlungen zu der jeweiligen Schutzstufe, bei der eine einheitliche Beurteilung vorgenommen werden kann, ist von einem damit besonders betrauten Mitarbeiter (ggf. dem Datenschutzbeauftragten) der entsprechenden Behörde vorzunehmen.

§ 10

(1) Die Zuordnung personenbezogener Sammlungen mit Vorgängen verschiedener Schutzstufen soll vom zuständigen Sachbearbeiter vorgenommen werden.

(2) Der mit diesen Angelegenheiten besonders betraute Mitarbeiter (ggf. der Datenschutzbeauftragte) ist über die Zuordnung zu informieren.

§ 11

Ausschlaggebend für die Zuordnung personenbezogener Sammlungen ist die Schutzstufe, der die Mehrzahl der in ihnen enthaltenen personenbezogenen Daten unterliegt.

§ 12

(1) Enthält eine personenbezogene Sammlung Einzelvorgänge, die einer höheren Schutzstufe unterliegen als die Sammlung, so sind diese Vorgänge gesondert zuzuordnen.

(2) Das gleiche gilt für Teile von Vorgängen.

V. Kennzeichnung

§ 13

Vertrauliche Vorgänge sind äußerlich sichtbar mit dem Vermerk "vertraulich" zu versehen.

§ 14

Streng vertrauliche Vorgänge sind äußerlich sichtbar mit dem Vermerk "streng vertraulich" zu versehen.

§ 15

Weicht die Zuordnung vertraulicher oder streng vertraulicher Teilvorgänge von der Zuordnung des Vorganges ab, dann sind die Teilvorgänge zu kennzeichnen.

VI. Aufbewahrung

§ 16

Es ist sicherzustellen, daß unbefugten Personen keine geschützten Daten offenbart werden. Diensträume, in denen sich geschützte Vorgänge befinden, sind, wenn sie - auch nur kurzzeitig - nicht besetzt sind, zu verschließen.

a) Aufbewahrung während des Geschäftsganges

§ 17

Geschützte Vorgänge sind außerhalb der Geschäftszeiten in verschlossenen Räumen oder verschlossenen Behältnissen, die keinen zufälligen Zugriff erlauben, zu verwahren.

§ 18

Vertrauliche Vorgänge sind in verschlossenen Schränken, die sich in abschließbaren Räumen befinden, aufzubewahren.

§ 19

Streng vertrauliche Vorgänge müssen darüber hinaus in Behältnissen aufbewahrt werden, bei denen ein unbefugtes Öffnen ohne sichtbare Gewaltanwendung nicht möglich ist.

b) Aufbewahrung von Altvorgängen

§ 20

Altvorgänge sind entsprechend oder in besonders gesicherten Räumen aufzubewahren. Der Personenkreis, der Zugang zu solchen Daten oder Räumen hat, in denen sich Vorgänge mit solchen Daten befinden, ist begrenzt zu halten und namentlich festzustellen.

c) Teilvorgänge

§ 21

Befinden sich einzelne vertrauliche Teilvorgänge in geschützten Vorgängen oder streng vertrauliche Teilvorgänge in vertraulichen oder geschützten Vorgängen, so sind diese in einem versiegelten Umschlag in den Vorgängen aufzubewahren.

VII. Zugriff

§ 22

(1) Zugriff zu Daten aller Schutzstufen hat grundsätzlich nur der zuständige Sachbearbeiter.

(2) Außer dem zuständigen Sachbearbeiter hat folgender Personenkreis im Rahmen seines Verantwortungsbereiches Zugriff:

1. zu offenen Daten:
   a) Schreibkräfte,
      soweit notwendig auf Anweisung eines Berechtigten (Abs. 1 und 2 Nr. 4) auch bis streng vertrauliche Daten,
   b) Betriebspraktikanten;
2. bis zu geschützten Daten:
   a) Beamtenanwärter und Auszubildende,
      wenn für die Ausbildung förderlich auch vertrauliche und sofern notwendig auch streng vertrauliche Daten,
   b) Fachoberschulpraktikanten,
      wenn für die Ausbildung förderlich auch vertrauliche Daten;
3. bis zu vertraulichen Daten:
   a) Büroleiter,
      mit Zustimmung der Berechtigten (Abs. 1 und 2 Nr. 4) auch streng vertrauliche Daten,
   b) Zuarbeiter,
      mit Zustimmung der Berechtigten (Abs. 1 und 2 Nr. 4) auch streng vertrauliche Daten;

4. bis zu streng vertraulichen Daten:
   a) Büroleiter,
   b) Dienstkräfte mit Leitungsaufgaben,
   c) der für den Datenschutz beauftragte Mitarbeiter für seine Aufgaben.

VIII. Transport von Daten

a) Innerdienstlicher Transport

§ 23

Geschützte Daten sind in Umlaufmappen zu transportieren. Die Umlaufmappen brauchen nicht verschlossen zu sein, wenn durch organisatorische Maßnahmen gewährleistet ist, daß Unbefugte keine Einsicht nehmen können.

§ 24

(1) Vertrauliche Daten dürfen nur verschlossen transportiert werden. Der Umschlag muß die Aufschrift "vertraulich" erhalten, so daß er von den Postverteilungsstellen nicht geöffnet wird. Nach Möglichkeit ist der Umschlag auch mit dem Namen oder dem Stellenzeichen des Empfängers zu versehen.

(2) Der innerdienstliche Botenverkehr ist ausreichend.

(3) Innerhalb eines Dienstgebäudes ist der unverschlossene Transport dieser Daten durch den entsprechenden Sachbearbeiter zulässig.

§ 25

(1) Der Schutz streng vertraulicher Daten unterliegt einer besonderen Sorgfaltspflicht durch den Sachbearbeiter.

(2) Streng vertrauliche Daten sind nur in verschlossenen und versiegelten Umschlägen und mit der Aufschrift "streng vertraulich" durch Boten gesondert zu transportieren. Dabei ist der Empfang der Daten durch Empfangsbekenntnis zu kontrollieren. Ist kein direkter Empfänger bekannt, so sind die Daten dem Behördenleiter zuzusenden.

(3) Die Mitnahme von streng vertraulichen Daten durch den Sachbearbeiter außerhalb des eigenen Dienstgebäudes der Berliner Verwaltung darf nur in verschließbaren Aktenkoffern erfolgen.

b) Außerdienstlicher Transport

§ 26

Geschützte und vertrauliche Daten sind verschlossen zu versenden. Postkarten sind nur für Vorladungen oder Bitten um Anruf zu verwenden. Lassen sich nähere Angaben über die Angelegenheit nicht vermeiden, ist die Postkarte ebenfalls verschlossen zu versenden.

§ 27

(1) Streng vertrauliche Daten sind so zu versenden, daß sichergestellt ist, daß nur der Empfänger selbst das Schriftstück erhält.

(2) Der verschlossene Brief ist entweder durch Boten oder auf dem Postwege mit Postzustellungsurkunde zuzustellen. Die Postzustellungsurkunde ist mit dem Vermerk „nur dem Empfänger persönlich auszuhändigen" zu versehen. Wird der Brief durch einen Boten überbracht, so hat dieser sich von der Identität des Empfängers zu überzeugen.

IX. Auskunft

a) Telefonische Auskunft

§ 28

(1) Offene Daten dürfen jederzeit ohne Prüfung der Empfangsberechtigung übermittelt werden, sofern der Anfragende geltend macht, die Daten zu benötigen.

(2) Die Übermittlung zu Werbe- und Vermarktungszwecken ist unzulässig.

§ 29

(1) Geschützte Daten dürfen an Privatpersonen oder deren legitimierte Vertreter nur übermittelt werden, wenn über die Berechtigung und die Identität des Anfragenden keine Zweifel bestehen.

(2) An öffentliche Stellen ist die Übermittlung nur zulässig, wenn keine Zweifel bestehen, daß die Daten zur rechtmäßigen Aufgabenerfüllung der anfragenden Stelle erforderlich sind.

§ 30

(1) Vertrauliche Daten dürfen an Privatpersonen oder deren legitimierte Vertreter nur übermittelt werden, wenn die Berechtigung und die Identität des Anfragenden sichergestellt sind.

(2) An öffentliche Stellen ist die Übermittlung nur zulässig, wenn sichergestellt ist, daß die Angaben zur rechtmäßigen Aufgabenerfüllung der anfragenden Stelle erforderlich sind. Die Identität des Nachfragenden muß feststehen.

(3) Über den Inhalt der Auskunft, die Berechtigung und die Identität des Anfragenden ist ein Vermerk zu fertigen.

§ 31

Streng vertrauliche Daten dürfen telefonisch nicht übermittelt werden.

b) Schriftliche Auskunft

§ 32

Für offene Daten gilt § 28 entsprechend.

§ 33

(1) Geschützte Daten dürfen an Privatpersonen oder deren legitimierte Vertreter übermittelt werden, wenn über die Berechtigung keine Zweifel bestehen.

(2) An öffentliche Stellen ist die Übermittlung nur zulässig, wenn keine Zweifel bestehen, daß die Daten zur rechtmäßigen Aufgabenerfüllung erforderlich sind.

§ 34

(1) Vertrauliche Daten dürfen an Privatpersonen oder deren legitimierte Vertreter nur übermittelt werden, wenn die Berechtigung sichergestellt ist.

(2) An öffentliche Stellen ist die Übermittlung nur zulässig, wenn sichergestellt ist, daß die Angaben zur rechtmäßigen Aufgabenerfüllung erforderlich sind.

§ 35

(1) Streng vertrauliche Daten dürfen an Privatpersonen oder deren legitimierte Vertreter nur übermittelt werden, wenn eine schriftliche Anfrage vorliegt und die Berechtigung sichergestellt ist.

(2) An öffentliche Stellen ist die Übermittlung nur zulässig, wenn schriftlich nachgewiesen ist, daß die Daten zur rechtmäßigen Aufgabenerfüllung unbedingt erforderlich sind.

c) Einsichtnahme

§ 36

(1) Für die Einsichtnahme in Vorgänge (z. B. Akteneinsicht) in den Diensträumen gelten die §§ 28 bis 30 entsprechend.

(2) Die Einsicht in streng vertrauliche Vorgänge ist nur zulässig, wenn ein schriftlicher Antrag vorliegt und Berechtigung und Identität des Einsichtnehmenden sichergestellt sind. Über die Einsichtnahme ist ein Vermerk zu fertigen.

(3) Für den Versand von Vorgängen zum Zwecke der Einsichtnahme gelten die §§ 32 bis 35.

d) Einwilligung

§ 37

(1) Auf Grund einer schriftlichen Einwilligung desjenigen, über den personenbezogene Daten vorliegen, können diese auch an Dritte übermittelt werden.

(2) Die Einwilligung soll auf bestimmte Daten und Personen beschränkt und kann befristet werden.

(3) Die Einwilligung bedarf nicht der Schriftform, wenn wegen besonderer Umstände eine andere Form der Einwilligung angemessen ist. Dies gilt nicht für vertrauliche und streng vertrauliche Daten.

X. Vernichtung

§ 38

Schriftstücke und sonstige Datenträger, die offene Daten enthalten, können unmittelbar der Wiederverwertung zugeführt werden.

§ 39

(1) Enthalten Schriftstücke und sonstige Datenträger geschützte oder vertrauliche Daten, so sind diese vor der Wiederverwertung mit dem Aktenwolf zu vernichten. Ist dies nicht möglich, sind sie zu bündeln und der Müllverbrennungsanlage zu übergeben. Dabei ist sicherzustellen, daß keine einzelnen Schriftstücke entnommen werden können.

(2) Darüber hinaus hat die Vernichtung von Schriftstücken und sonstigen Datenträgern, die streng vertrauliche Daten enthalten, in Anwesenheit eines Zeugen zu erfolgen und ist schriftlich festzuhalten.

(3) Abfälle, insbesondere Zwischenmaterial, sind so zu vernichten, daß eine Einsichtnahme durch Unbefugte ausgeschlossen bleibt.

Anlage 3

Stichwortverzeichnis zu den seit 1979 erschienenen Jahresberichten

Zitierweise: **Jahr**, Seite **79**, 14 = 1979, S. 14