

**Der Bayerische Landesbeauftragte
für den Datenschutz**

18. Tätigkeitsbericht, 1998

Stand: 16.12.1998

1. Neuer Standort des Datenschutzes in Europa

Mein 18. Tätigkeitsbericht steht unter dem gleichen Motto wie mein vorheriger Tätigkeitsbericht:

Datenschutz ist Grundrechtsschutz..

Dieses Motto erhält jetzt zusätzliches Gewicht dadurch, daß durch die Änderung der Bayerischen Verfassung vom 20. Februar 1998 die Institution Landesbeauftragter für den Datenschutz in die Bayerische Verfassung aufgenommen wurde.

Nach Art. 33a BV, der zum Teil am 1. März, zum Teil am 1. Oktober dieses Jahres in Kraft getreten ist,

- wird der Landesbeauftragte in Zukunft vom Landtag auf Vorschlag der Staatsregierung auf die Dauer von 6 Jahren gewählt, anstatt wie bisher von der Staatsregierung mit Zustimmung des Landtags auf die Dauer von 8 Jahren berufen,
- untersteht er der Dienstaufsicht des Präsidenten des Bayerischen Landtags, anstatt wie bisher der Dienstaufsicht des Ministerpräsidenten,
- kann er nur, wenn eine entsprechende Anwendung der Vorschriften über die Amtsenthebung von Richtern auf Lebenszeit dies rechtfertigt, mit Zwei-Drittel Mehrheit abberufen werden.
- Ebenfalls in die Verfassung aufgenommen wurde die Kontrollaufgabe des Landesbeauftragten, **allerdings** "nach Maßgabe des Gesetzes".
-

Nach der zur Ausführung dieser neuen Verfassungsbestimmung ergangenen Änderung des Bayerischen Datenschutzgesetzes vom 10. Juli 1998 ist meine Geschäftsstelle seit 1. Oktober dieses Jahres anstatt wie bisher bei der Staatskanzlei in Zukunft beim Bayerischen Landtag eingerichtet.

Ich sehe in diesen Änderungen eine Stärkung der Stellung des Bayerischen Landesbeauftragten für den Datenschutz. Durch die Aufnahme der Institution des Datenschutzbeauftragten und seiner Kontrollaufgabe in die Verfassung wird der Schutz des Rechts auf informationelle Selbstbestimmung als verfassungswerte Institution von der Bayerischen Verfassung anerkannt. Eine

Ausweitung der Kontrollzuständigkeit ist wegen des Gesetzesvorbehalts damit zwar nicht verbunden, die Problematik der Einschränkung meiner Kontrollbefugnis in Akten auf Vorgänge, für die ich einen Anlaß zur Kontrolle habe, besteht nach wie vor (vgl. dazu unten [Nr. 1.5](#)). Ich meine aber, daß die Aufnahme der Institution des Datenschutzbeauftragten in die Verfassung ihr ein größeres und nach den Ausführungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil auch zukommendes Gewicht gibt. Das Bundesverfassungsgericht hat dort betont, daß die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung ist.

Ich verspreche mir von der Aufnahme in die Verfassung und der Zuordnung zum Landtag auch eine bessere Anerkennung des Landesbeauftragten als regierungsferne Kontrollinstitution. Zur rechtlichen und tatsächlichen Stärkung der Unabhängigkeit war die Änderung zwar nicht nötig - die Unabhängigkeit war auch unter der bisherigen Rechts- und Sachlage in vollem Umfang gegeben - das Bild nach außen als Kontrollorgan ist mit der Herausnahme aus dem Bereich der Staatskanzlei und mit der Zuordnung zum Landtag, dem ja auch die Kontrolle der Regierung obliegt, aber jetzt deutlicher.

1.1 Neue Aufgaben für den Datenschutz

Schon in meinem [17. Tätigkeitsbericht](#) habe ich darauf hingewiesen, daß sowohl die technische als auch die organisatorische Entwicklung, wie auch die gestiegenen Bedürfnisse nach Datenverarbeitung auch den Datenschutz vor neue Aufgaben stellen. Diese Entwicklung hat sich fortgesetzt. Datenverarbeitung ist immer mehr dezentral, vernetzt und - auch im öffentlichen Bereich - international. Der Umfang der Datenverarbeitung steigt auch mit wachsendem Bedarf nach Sicherheit und mit wachsenden Kontrollanforderungen gegen Mißbräuche des Sozialleistungswesens.

Aufgabe des Datenschutzes in diesem veränderten Feld ist es zu gewährleisten, daß in die Rechte der **Bürger nur soweit eingegriffen wird, als das zur Erfüllung der öffentlichen Aufgaben erforderlich ist und nur soweit, als das im Licht des Grundrechts auf informationelle Selbstbestimmung auch verhältnismäßig ist.** Wenn von Seiten des Datenschutzes in Erfüllung

dieser Aufgabe Forderungen nach Begrenzung oder Umgestaltungen erhoben werden, dann darf das nicht mit **der Kampfparole "Datenschutz ist Täterschutz" abgewehrt werden**, auch deswegen nicht, weil recht verstandener Datenschutz auch die berechtigten Bedürfnisse der Verwaltung in seine Beurteilung einbezieht. Es ist aber Aufgabe des Datenschutzes, auf die Grenzen hinzuweisen, die sich aus den verfassungsrechtlichen Prinzipien der Erforderlichkeit und der Verhältnismäßigkeit, sowie aus den gesetzlichen Datenverarbeitungsbegrenzungen ergeben, und auf die Einhaltung dieser Grenzen hinzuwirken. Das sollte nicht in dieser Weise desavouiert werden.

Seine Aufgaben wird der Datenschutzbeauftragte auch in Zukunft jedenfalls auch im Weg der nachträglichen Kontrollen erfüllen müssen. Daß dadurch zahlreiche Schwachpunkte aufgezeigt werden, lege ich in diesem Bericht im einzelnen und in diesem Abschnitt in einem kurzen Überblick dar. Ich bin deshalb skeptisch gegen Forderungen in der datenschutzrechtlichen Diskussion, daß man von der großen Gewichtung der Kontrollen wegkommen müsse.

Datenschutz darf sich aber nicht nur als reine Kontrolleinrichtung verstehen. Datenschutz ist vielmehr in wesentlicher Hinsicht **Dienstleistung am Bürger**. Die Institution Datenschutzbeauftragter ist deshalb Kontrollinstanz, aber genauso ein **"Dienstleistungsbetrieb Datenschutz"**. Dieser "Dienstleistungsbetrieb Datenschutz" soll **Anwalt des Bürgers und kritischer Partner der Verwaltung** sein. Der "Dienstleistungsbetrieb Datenschutz" kommt auch der Verwaltung zu Gute. Durch **rechtzeitige Beratung** bei der datenschutzrechtlichen Gestaltung von Verwaltungsabläufen können sichere und datenschutzrechtlich akzeptable Verfahrensweisen gefunden werden, die die Bedürfnisse der Verwaltung erfüllen und die Rechte der Bürger wahren. Sie tragen dadurch auch zur besseren Akzeptanz dieser Abläufe durch den Bürger bei. Sie können als **"vertrauensbildende Maßnahmen"** angesehen werden. Beispiele sind u.a. Forschungsvorhaben, Gesundheitsuntersuchungen ("Neugeborenen-Screening") und Nachweise früherer Behandlungen zur Anerkennung einer beruflichen Qualifikation (Approbation von Psychologen nach dem Psychotherapeutengesetz).

Im Zusammenhang mit dem Stichwort "Neue Aufgaben" nenne ich auch die **Umsetzung der [EG-Datenschutzrichtlinie](#)**. Sie wäre bis Oktober 1998 durchzuführen gewesen. Dieses ist so-

wohl im Bund, wie in Bayern nicht erfolgt. Die EG-Datenschutzrichtlinie wird im privaten Bereich weitergehende Änderungen bedingen als im öffentlichen Bereich. Aber auch im öffentlichen Bereich wird zu prüfen sein, inwieweit die Bürgerrechte, insbesondere Widerspruchs-, Informations- und Auskunftsrechte, sowie die Regelungen über den Umgang mit sensiblen Daten, im Hinblick auf die Richtlinie zu verbessern sind.

Die Umsetzung der EG-Richtlinie muß vor allem auch Anlaß sein, im neuen Datenschutzrecht auf die **Entwicklungen der vergangenen 20 Jahre** einzugehen. So sind Regelungen für Chipkartenanwendungen (z.B. über die datenschutzrechtliche Verantwortlichkeit und die Rechte des Karteninhabers, z.B. in Bezug auf Freiwilligkeit und Transparenz) genauso notwendig, wie für Voraussetzungen, Umfang und Grenzen der Videoüberwachung. In das neue Datenschutzrecht sind auch **Prinzipien modernen Datenschutzes** aufzunehmen, durch die der **Anfall personenbezogener Daten von vornherein minimiert werden soll**, wie der Grundsatz der **Datensparsamkeit, die Möglichkeit der Anonymisierung und das Verwenden von Pseudonymen**. Diese Forderungen, die den Begriff der Erforderlichkeit spezifizieren und nicht seinetwegen überflüssig sind, sind im neuen [Teledienstedatenschutzgesetz](#) und im [Mediendienstestaatsvertrag](#) enthalten und können als Modell für eine moderne Datenschutzregelung dienen.

1.2 Übersicht über meine Tätigkeit im Berichtszeitraum

(anhand einer Auswahl wesentlicher Einzelfeststellungen)

1. Im Bereich **Polizei** habe ich in nicht geringer Anzahl Mängel festgestellt.
Exemplarisch nenne ich hier:
 - a. **Im Landeskriminalaktennachweis** (vgl. [Nr. 5.3.1](#) dieses Tätigkeitsberichts), in dem 1,37 Mio. Personendatensätze (erster Platz unter den Flächenländern) enthalten sind,
 - erfolgt bei Verfahrenseinstellung durch die Staatsanwaltschaft seitens der Polizei regelmäßig **keine Einzelfallprüfung**, ob die Weiterspeicherung zur Kriminalitätsbekämpfung notwendig ist,

- werden die im Gesetz vorgesehenen **Höchstspeicherfristen als Regelfristen** mißverstanden,
- werden entgegen der Rechtsprechung seit 1996 die Speicherfristen nicht für jeden Fall gesondert festgelegt, sondern **jeweils nach der längsten Speicherung**;

Ich habe das Innenministerium aufgefordert, diese Verfahrensweise zu ändern.

- b. In der Datei "Pkw-Aufbrüche/Einbruchsdiebstähle" (vgl. [Nr. 5.4.3](#) dieses Tätigkeitsberichts) eines Polizeipräsidiums werden nicht nur Beschuldigte, sondern auch **nicht belastete Mitteleiler und Anzeigerstatter genauso 10 Jahre Mitteleiler und Anzeigerstatter genauso 10 Jahre** gespeichert; das Staatsministerium des Innern hat dies wegen einer seiner Ansicht nach erfahrungsgemäß möglichen Beteiligung der Genannten gerechtfertigt; ich habe das als unzulässige Datenspeicherung auf Vorrat kritisiert und eine Verkürzung der Speicherfristen auf das zur Sachbearbeitung Notwendige gefordert.
- c. Bei einem Polizeipräsidium werden **erkennungsdienstliche Maßnahmen** (Polaroidphotos; vgl. [Nr. 5.5.6](#) dieses Tätigkeitsberichts) gegen Personen durchgeführt, die auf Grund von einzelnen Erkennungsmerkmalen (z.B. punkerartige Kleidung, Besuch einschlägiger Lokale) bestimmten delinquenten Gruppierungen zugeordnet werden, ohne daß die gesetzlichen Voraussetzungen (Beschuldigter in einem Strafverfahren oder sonstiger konkreter Verdacht einer Straftat) vorlägen. Das Polizeipräsidium vertritt die Auffassung, daß die letztgenannte Voraussetzung bereits mit der o.g. Zuordnung zu einer solchen Gruppierung, aus der heraus Straftaten begangen wurden, erfüllt ist. Ich halte diese Auffassung für nicht vertretbar.

Unsere Prüfungen haben aber auch in weiten Bereichen keine datenschutzrechtlichen Mängel ergeben; so habe ich z.B. bei der Prüfung der Datenverarbeitung im Zusammenhang mit elektronischen Überwachungsmaßnahmen nach dem Polizeiaufgaben-

gesetz (vgl. [Nr. 5.5.2](#) dieses Tätigkeitsberichts) und von Telephonüberwachungsmaßnahmen nach der Strafprozeßordnung (vgl. [Nr. 5.5.3](#) dieses Tätigkeitsberichts) keine grundsätzlichen Mängel festgestellt.

2. Im Bereich **Datenverarbeitung im Sozialwesen** haben mich unter anderem die Grenzen der Datenübermittlungsbefugnisse zwischen Sozialämtern und Polizei, die Datenabgleichsmöglichkeiten zur Mißbrauchskontrolle und die Frage des Einsatzes von Sozialhilfermittlern sehr beschäftigt.
 - a. Da § 68 des X. Buches des Sozialgesetzbuches in der bisherigen, inzwischen allerdings geänderten Fassung, u.a. nur die **Übermittlung "der derzeitigen Anschrift" an die Polizei** zugelassen hatte, mußte ich eine weitergehende Weisung des Arbeits- und Sozialministeriums beanstanden (vgl. [Nr. 4.5.3](#) dieses Tätigkeitsberichts). Entgegen diesem für mich klaren Wortlaut forderte die Weisung zur Ermittlung von durch die Polizei Gesuchten, daß die **Sozialämter der Polizei auch Mitteilung über zukünftige Vorsprachetermine** machten. Die Weisung sollte es ermöglichen, daß die Gesuchten dann bei der Vorsprache beim Sozialamt von der Polizei festgenommen werden können. Mein Hinweis, daß solche Mitteilungen nur u.a. bei Ermittlungen wegen Sozialhilfebetrug und mit richterlicher Genehmigung bei Straftaten von erheblicher Bedeutung zulässig seien, brachte keine Änderung der Weisung. Ich habe mich daraufhin entsprechend dem Bayerischen Datenschutzgesetz an die Staatsregierung und den Landtag gewandt. Diese haben die Weisung des Arbeits- und Sozialministeriums bestätigt.

Der Vorgang zeigt exemplarisch die begrenzten Einflußmöglichkeiten des Datenschutzbeauftragten.

Inzwischen wurde die genannte Bestimmung auf die Übermittlung auch "**des künftigen Aufenthalts**" erweitert, um die genannten Auskünfte zu ermöglichen.

- b. Ein weiterer Schwerpunkt im Bereich Datenverarbeitung im Sozialwesen war die Frage, welche **Datenabgleichsmöglichkeiten zur Mißbrauchskontrolle** zusätzlich zu den vorhandenen Möglichkeiten erforderlich seien.

Hier hatte eine Arbeitsgruppe der Arbeits- und Sozialministerkonferenz eine Vorlage erarbeitet, die über die gegebenen Möglichkeiten hinaus **wesentliche Erweiterungen der Kontroll- und Abgleichsmöglichkeiten** auch ohne einen konkreten Mißbrauchsverdacht forderte (vgl. [Nr. 4.2](#) dieses Tätigkeitsberichts).

Dazu hat die Datenschutzkonferenz entsprechend einem Vorschlag ihres unter meiner Leitung stehenden Arbeitskreises "Gesundheit und Soziales" u.a. gefordert, daß vor der Einführung neuer Kontrollmechanismen, die das bisherige ausgewogene System von Kontrollmöglichkeiten sprengen würden, die bestehenden Kontrollmechanismen ausgeschöpft werden, die sehr wohl die erforderlichen Prüfungen auf das Vorliegen der Leistungsvoraussetzungen und auch bestimmte Datenabgleiche zulassen (vgl. [Anlage 9](#) zu diesem Tätigkeitsbericht).

Die Arbeits- und Sozialministerkonferenz hat in ihren Beschluß beide Vorlagen aufgenommen.

- c. Zu den **Sozialhilfeermittlern** (vgl. Nr. [4.5.4](#) dieses Tätigkeitsberichts) habe ich festgestellt, daß ihr Einsatz erst in Frage kommt, wenn andere, weniger eingreifende Maßnahmen ausgeschöpft sind, daß sie gegenüber dem Betroffenen offen auftreten müssen, daß sie sich keinen Zutritt zur Wohnung erzwingen oder erschleichen dürfen, daß bei der Befragung von Dritten besondere Zurückhaltung zu üben ist und daß gegen eine verdeckte Beobachtung größte Bedenken bestehen.
3. Im **Gesundheitswesen** hebe ich die Themen Datenschutz und Forschungsfreiheit, datenschutzfreundliche Gestaltung von Befähigungsnachweisen nach dem Psychotherapeutengesetz und die datenschutzgerechte Einrichtung von klinischen Informationssystemen hervor.

- a. Bei **Forschungsvorhaben** ist es mir ein wesentliches Anliegen, sowohl dem informationellen Selbstbestimmungsrecht, wie auch dem Grundrecht auf Forschungsfreiheit gerecht zu werden. Beide Grundrechte müssen im Sinn der **praktischen Konkordanz zu einer Optimierung** gebracht werden.

Gespräche mit der **Deutschen Arbeitsgemeinschaft für Epidemiologie** (vgl. [Nr. 2.3.1](#) dieses Tätigkeitsberichts) haben gezeigt, daß sich über die Anonymisierung und Pseudonymisierung, erforderlichenfalls die informierte Einwilligung des Betroffenen und die praxisgerechte Auslegung der gesetzlichen Bestimmungen in aller Regel Ergebnisse erzielen lassen, die sowohl der Forschung, wie auch dem Datenschutz gerecht werden. Beispiele schildere ich nachstehend in meinem Bericht.

Das schließt nicht aus, daß noch Regelungsbedarf besteht. So habe ich in meinem Referat bei dem 7. Wiesbadener Datenschutzforum (vgl. [Nr. 2.3.2](#) dieses Tätigkeitsberichts) zum Thema Datenschutz und Forschungsfreiheit in Frage gestellt, ob die übliche Formulierung in den Forschungsklauseln der Landesdatenschutzgesetze, wonach für die Übermittlung personenbezogener Daten zu Forschungszwecken das Forschungsinteresse das Recht auf informationelle Selbstbestimmung **erheblich** überwiegen müsse, mit dem **Grundrecht der Forschungsfreiheit** vereinbar sei. Ich habe zu überlegen gegeben, ob nicht im Hinblick auf die Grundrechtskonkurrenz ein einfaches Überwiegen des Forschungsinteresses im konkreten Fall genügen müsse. Es hat mich sehr gefreut, daß der Hessische Landesgesetzgeber meinen Hinweis bei der Novellierung des Hessischen Datenschutzgesetzes aufgegriffen und das Wort "erheblich" gestrichen hat.

- b. Die für die Approbation von Psychologen zu Psychotherapeuten (vgl. [Nr. 3.2](#) dieses Tätigkeitsberichts) nach dem neuen Psychotherapeutengesetz vorzulegenden **Tätigkeitsnachweise** sollten **ursprünglich nicht anonymisiert** werden. Das

hätte die Vorlage von höchst sensiblen medizinischen Informationen völlig unbeeiligtter Dritter an die Genehmigungsbehörden bedeutet. Hier konnte ich durch entsprechende Hinweise des Arbeitskreises Gesundheit und Soziales der Datenschutzkonferenz erreichen, daß das Arbeits- und Sozialministerium inzwischen die regelmäßig anonymisierte Vorlage der Tätigkeitsnachweise vorsieht.

- c. Besonderes Gewicht habe ich auch der Frage der **datenschutzgerechten Gestaltung von Klinikinformationssystemen** (vgl. [Nr. 3.3.2](#) u. [3.3.3](#) dieses Tätigkeitsberichts) beigemessen. Inzwischen werden in diesen Systemen nicht mehr nur Verwaltungsdaten, sondern auch medizinische Daten verarbeitet. Zur Wahrung des informationellen Selbstbestimmungsrechts des Patienten, aber auch des Arztgeheimnisses ist es notwendig, daß die Zugriffsrechte auf die Patientendaten nur entsprechend den Behandlungserfordernissen eingeräumt und begrenzt werden. Ich gehe dieser Frage gerade bei einer noch nicht abgeschlossenen Prüfung eines Münchner Krankenhauses nach, in dem ein System differenzierter Zugriffsberechtigungen eingerichtet wird. Ich werde diese Frage auch in anderen Krankenhäusern aufgreifen.

4. Im Bereich **Kommunen, Einwohnermeldewesen** waren u.a. Fragen des Inhalts und der Auswertung von Eintragungslisten für Volks- und Bürgerbegehren, der unbefugten Übermittlung von Informationen aus nichtöffentlichen Sitzungen und Unterlagen an die Presse, der Herausgabe von Adressenlisten für kommunalfremde Zwecke, der Weitergabe von Meldedaten an Adreßbuchverlage und Parteien sowie der Videoüberwachung relevant.
 - a. Zum Inhalt der **Eintragungslisten für Volks- und Bürgerbegehren** (vgl. [Nr. 8.3](#) u. [8.4.1](#) dieses Tätigkeitsberichts) habe ich u.a. vorgeschlagen, auf das Geburtsdatum zu verzichten, da es m.E. für den Identitätsnachweis i.d.R. überflüssig ist. Unzulässige Auswertungen und Einsichtnahmen in Eintragungslisten für Bürgerbegehren mußte ich rügen (vgl. [Nr. 8.4.2](#) dieses Tätigkeitsberichts).

- b. Mehrfach mußte ich in einem Fallkomplex die **unbefugte Erhebung und Weitergabe von Informationen aus nichtöffentlichen Schriftstücken** beanstanden (vgl. [Nr. 8.10](#) u. [8.11](#) dieses Tätigkeitsberichts). Der Fall ist besonders bemerkenswert, da die betroffene Kommune alles unternimmt, um die Informationsweitergabe abzustellen und ich mich gleichwohl inzwischen mit der vierten Beschwerde in der Angelegenheit befassen muß. Hier bleibt letztlich nur noch der Ruf nach dem Staatsanwalt.
- c. Die Herausgabe von **Meldedaten an Parteien und Adreßbuchverlage** war mehrfach Gegenstand von Bürgerbeschwerden (vgl. [Nr. 9.1](#) dieses Tätigkeitsberichts). Ich habe dazu zwar keine Verletzung des geltenden Rechts festgestellt, wegen der offensichtlichen Wirkungslosigkeit des gegenwärtigen Widerspruchsverfahrens - wohl auch auf Grund mangelhafter Information der Bürger - habe ich mich in der letzten Datenschutzkonferenz aber in einer Entschlieung dafür eingesetzt, daß die derzeitige Widerspruchslösung durch eine Einwilligungslösung ersetzt wird.
- d. Immer wieder zu Anfragen führt auch die **Videoüberwachung von öffentlichen Plätzen** zur Abwehr und Verfolgung von Ordnungswidrigkeiten und Straftaten (vgl. [Nr. 18.1](#) dieses Tätigkeitsberichts). Ich habe für die Videoüberwachung kommunaler Wertstoffhöfe und von Containerstandorten auf der Grundlage des Bayer. Datenschutzgesetzes festgestellt, daß dagegen keine Bedenken bestehen, wenn auf die Überwachung hingewiesen und eine Auswertung nur vorgenommen wird, wenn unerlaubte Ablagerungen festgestellt werden. Gleichwohl halte ich den Komplex Videoüberwachung für regelungsbedürftig, wie ich eingangs ausgeführt habe.
5. Im Bereich "**Technik und Organisation**" wurden zahlreiche Beratungen und Prüfungen durchgeführt. Gerade in diesem Bereich ist die frühzeitige Beratung über technische und organisatorische Sicherungsmaßnahmen besonders wichtig und wird von unseren Kun-

den auch gerne in Anspruch genommen. Dabei geht es nicht nur um Einzelfragen, sondern besonders um technische Grundsatzfragen, wobei ich auszugsweise auf folgende Punkte hinweisen möchte:

- a. **Datenschutzfreundliche Technologien** (vgl. [Nr. 19.1.3](#) dieses Tätigkeitsberichts), durch die den Grundsätzen der Datensparsamkeit und womöglich der Datenvermeidung Rechnung getragen werden kann,
- b. **Einsatz kryptographischer Verfahren** (vgl. [Nr. 19.1.4](#) dieses Tätigkeitsberichts) zur Sicherstellung von Vertraulichkeit, Integrität und Authentizität - besonders wichtig wegen der systembedingten Unsicherheiten - wobei ich wegen der mangelnden Effektivität und der Sicherheitsprobleme Schlüsselhinterlegungs- und Wiedergewinnungsverfahren ablehne- und die
- c. **Sicherheitsaspekte bei der Nutzung des Internets** (vgl. [Nr. 19.1.5](#) dieses Tätigkeitsberichts), die einerseits umfangreiche Datenspuren im Netz erzeugt, und die andererseits die Gefahr von Angriffen aus dem Netz auf den eigenen Rechner und die übertragenen Daten mit sich bringt, und denen unter den Stichworten Systemdatenschutz, Selbstdatenschutz und technischer Datenschutz Rechnung getragen werden kann und muß.

Zu vorgenannten Punkten und zu anderen technischen und organisatorischen Fragen sind auf meiner **Homepage im Internet** unter der Adresse **www.datenschutz-bayern.de** zahlreiche Hinweise und Handreichungen einseh- und abrufbar.

Die technischen und organisatorischen Prüfungen haben im übrigen ergeben, daß bei allen Sparzwängen sich die meisten kontrollierten Dienststellen, einige in vorbildlicher Weise, bemühen Datenschutz und Datensicherheit zu gewährleisten, was einzelne Mängel nicht ausschließt.

Besonders erwähnen möchte ich das Bayerische Behördenetz (vgl. [Nr. 19.3.1](#) dieses Tätigkeitsberichts), für das umfangreiche technische und organisatorische Sicherheitsmaßnahmen gegen

Eindringversuche von außen und gegen Mißbräuche von innen getroffen wurden. Was noch aussteht, ist der flächendeckende Einsatz von Systemen, die eine vertrauliche und nicht manipulierbare Datenübertragung gewährleisten. Hierzu dient das Projekt BASILIKA, das aber noch nicht abgeschlossen werden konnte. Aus diesem Grund ist eine gegen unbefugte Kenntnisnahme und Veränderung gesicherte Datenübermittlung im Bayer. Behördennetz derzeit noch nicht gewährleistet, worauf ich mehrfach hingewiesen habe.

1.3 Stellungnahmen zu Normen und Richtlinien

Ich habe wieder zu zahlreichen Normen und Richtlinien Stellung genommen, wobei meinen Vorschlägen zum Teil Rechnung getragen wurde. Exemplarisch nenne ich:

- Zum Komplex **Zeugenschutzgesetz** haben wir Datenschutzbeauftragten in einer Entscheidung über die informationelle Selbstbestimmung bei Bild- und Tonaufzeichnungen im Strafverfahren Forderungen zum Schutz von Zeugen, insbesondere kindlichen Opferzeugen aufgestellt. Sie betrafen u.a. ein Verbot der Verfremdung, der justizfremden Verwendung und der Übermittlung an Stellen außerhalb der Justiz. Unsere Forderungen wurden mit dem Verbot der Verwendung für Zwecke außerhalb der Strafverfolgung teilweise berücksichtigt. Wegen der Mißbrauchsgefahren bedauere ich besonders das Fehlen eines Verbots der Vervielfältigung und der Versendung an Stellen außerhalb der Justiz.
- Zum sog. **Großen Lauschangriff** habe ich zusammen mit den anderen Datenschutzbeauftragten einen Forderungskatalog aufgestellt, von dem wichtige Forderungen offen blieben, u.a. nach Einschränkung des zu weiten Straftatenkatalogs und der Möglichkeit des Abhörens von Wohnungen Nichtbeschuldigter. Dagegen wurde in letzter Minute, wohl auch auf Grund der Appelle aller Datenschutzbeauftragten, das Abhören von Berufsheimnisträgern ausgeschlossen.
- Zur **DNA-Speicherung für polizeiliche Zwecke** haben wir Datenschutzbeauftragten bereits mehr als ein Jahr vor den jüngsten gesetzgeberischen Aktivitäten in einer Entscheidung festgestellt, daß eine derartige Speicherung unter bestimmten Voraussetzungen aus unserer Sicht möglich ist. Leider wurden diese Vorschläge nicht aufgegriffen. Statt des-

sen wurde zunächst ohne spezielle Rechtsgrundlage lediglich auf Grund einer Verwaltungsvorschrift eine derartige Datei eingerichtet. Unsere Forderungen nach einem speziellen Gesetz, in dem Speichervoraussetzungen und -dauer geregelt sind, in dem eine enge Zweckbindung (Verwendung ausschließlich zur Verfolgung von Straftaten und zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit) vorgesehen ist und in dem der Richtervorbehalt konsequent durchgeführt ist, sind auch im jetzt in Kraft getretenen DNA-Identitätsfeststellungsgesetz nicht berücksichtigt.

- **Verwaltungsvorschriften zum Justizmitteilungsgesetz:** Den Forderungen der Datenschutzbeauftragten nach Einführung der im Justizmitteilungsgesetz entgegen unserer Kritik nicht enthaltenen Richtervorbehalte für Mitteilungen aus Zivil und Strafverfahren an öffentliche Stellen wurde durch Einführung von Richter- und Staatsanwaltsvorbehalten in den Verwaltungsvorschriften z.T. Rechnung getragen.

1.4 Nationale und internationale Konferenzen

Im Jahr 1997 hatte ich **den Vorsitz in der Datenschutzkonferenz** des Bundes und der Länder. Es fanden zwei Sitzungen statt, die Frühjahrssitzung in München, die Herbstsitzung in Bamberg. Der würdige Rahmen der Sitzungen, u.a. Tagung der Herbstsitzung im Saal des historischen Brückenrathauses von Bamberg, fand bei den Teilnehmern sehr großen Anklang. Ich benutze diese Gelegenheit, mich bei der Staatsregierung für die großzügige Ausrichtung sehr herzlich zu bedanken. Dieser Dank gilt auch der Stadt Bamberg und insbesondere Herrn Oberbürgermeister Lauer für die Bereitstellung des Saales im historischen Brückenrathaus und den herzlichen Empfang.

Die Datenschutzbeauftragten haben Bayern in sehr guter Erinnerung.

In der Sache waren die Sitzungen erfolgreich: Es wurden Entschlüsse zu wichtigen aktuellen Fragen gefaßt, u.a. die oben bereits erwähnten Entschlüsse zur DNA-Datei für erkennungsdienstliche Zwecke und zur Video-Aufzeichnung im Strafverfahren, darüber hinaus zum erweiterten Schutz von Patientendaten und zur Notwendigkeit datenschutzfreundlicher Techno-

logien; daneben haben wir uns u.a. auch mit Fragen der Computer- und Telemedizin beschäftigt. In den beiden Konferenzen des Jahres 1998 wurden unter dem Vorsitz des hessischen Kollegen Prof. Dr. Hamm u.a. Entschließungen zu Datenschutzproblemen des digitalen Fernsehens und der Geldkarte. Diese und die weiteren Entschließungen sind im Anhang zu diesem Bericht abgedruckt und können von meiner Homepage heruntergeladen werden.

Weiter habe ich 1997 an der Internationalen Datenschutzkonferenz in Brüssel teilgenommen, in der unter anderem Fragen des unterschiedlichen Datenschutzes bei grenzüberschreitenden Datenflüssen, besonders in den Vereinigten Staaten, Datenerhebungen im Polizeibereich, insbesondere Schengen, Datenschutz im Internet und Datenschutz und Pressefreiheit diskutiert wurden. Wegen der globalen Natur der Datenverarbeitung ist der Blick über die Grenzen notwendig.

1.5 Rückblick auf den 17. Tätigkeitsbericht

Zwei Fragen aus meinem letzten Tätigkeitsbericht sollen am Schluß dieser Einführung stehen:

- **Der Bayer. Verfassungsgerichtshof ist in seiner Entscheidung vom 11. November 1997 zu meiner Kontrollkompetenz im Sicherheitsbereich** meiner These nicht gefolgt, daß für eine effektive Kontrolle von verdeckten Datenerhebungen eine externe Kontrolle durch den Datenschutzbeauftragten **auch bei nur in Akten verarbeiteten Daten ohne Anlaß** notwendig ist. Ich hatte das damit begründet, daß solche Erhebungen nicht in allen Fällen von Gerichten angeordnet werden und sie auch vom Betroffenen in der Regel mangels Kenntnis nicht einer Überprüfung zugeführt werden können. Eine externe Kontrolle durch den Landesbeauftragten für den Datenschutz der Datenverarbeitung in Akten würde nach der derzeitigen Gesetzeslage einen Anlaß voraussetzen, der sich mangels Beschwerden (Betroffener hat keine Kenntnis) in der Regel nicht ergeben wird. Eine externe Kontrolle solcher verdeckter Datenerhebungen ist also nur möglich, wenn das Anlaßfordernis wegfällt.

Das Gericht hat dies mit dem bisher nicht gehörten Argument abgelehnt, daß - sinngemäß - der Gesetzgeber den Datenschutzbeauftragten als Sicherheitsrisiko ansehen könne, und

weiter damit, daß auch verwaltungsinterne Kontrollen ausreichend seien. In einem Kommentar in einer Fachzeitschrift habe ich darauf hingewiesen, daß bei den unbestritten möglichen Dateikontrollen im Sicherheitsbereich derartige Sicherheitsrisiken auch nicht angenommen werden und daß externe Kontrollen gerade in diesem sensiblen Bereich notwendig sind.

Ich würde es sehr begrüßen, wenn der Gesetzgeber bei der Novellierung des Bayer. Datenschutzgesetzes durch Streichung dieser Beschränkung klarstellen würde, daß er auch hinsichtlich der Kontrolle nur in Akten den Datenschutzbeauftragten nicht als Sicherheitsrisiko ansieht.

- Für das **zentrale staatsanwaltschaftliche Verfahrensregister - STARIS** - ist das Staatsministerium der Justiz meiner Forderung gefolgt, für dieses ohne besondere Rechtsgrundlage eingeführte System die Begrenzungen des in der Strafprozeßordnung vorgesehenen bundesweiten, aber noch nicht eingerichteten Systems einzuhalten. Dementsprechend werden die Speicherungen 2 Jahre u.a. nach rechtskräftigen Freisprüchen gelöscht, eine Speicherung von Bußgeldverfahren erfolgt nicht.

Mit diesem kleinen Rückblick möchte ich den allgemeinen Teil meines 18.Tätigkeitsberichts beschließen und ihn der freundlichen Aufmerksamkeit des Bayer. Landtags, der Bayerischen Staatsregierung, des Bayerischen Senats und aller interessierten Leser empfehlen. Er ist auch als HTML- Dokument wiederum auf meiner Homepage im Internet veröffentlicht.

2. Allgemeines Datenschutzrecht

2.1 Datenschutzrecht in der Europäischen Union

Bereits mit ihrer EntschlieÙung in der 50. Konferenz vom 09./10. November 1995 (abgedruckt in meinem 17. Tätigkeitsbericht, [Anlage 2](#)) haben sich die Datenschutzbeauftragten des Bundes und der Länder die Forderung der Konferenz der Datenschutzbeauftragten der **Europäischen Union** zu eigen gemacht, anläÙlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen **Grundrechtskatalog** ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Ein solcher Katalog ist jedoch im Vertrag von Amsterdam (Maastricht II) vom 02. Oktober 1997 nicht enthalten.

Gefordert wurde ferner die Einführung eines für die **EU-Institutionen** verbindlichen eigenen Datenschutzrechts. Diese Forderung wurde teilweise realisiert: Gem. Art. 286 Abs. 1 des Vertrags von Amsterdam finden ab 01. Januar 1999 die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr solcher Daten auf die durch diesen Vertrag oder auf der Grundlage dieses Vertrags errichteten Organe und Einrichtungen der Gemeinschaft Anwendung. Dies bedeutet, daß unter anderem die **EG-Datenschutzrichtlinie** vom 24. Oktober 1995 ab dem 01. Januar 1999 auch auf die Einrichtungen und Organe der EU anwendbar ist. Eine Umsetzung der Richtlinie in verbindliche Datenschutzvorschriften für die Verwaltungsbehörden der EU steht noch aus. Ich hoffe, daß diese Vorschriften in naher Zukunft geschaffen werden.

2.2 Umsetzung der EG-Datenschutzrichtlinie

Die **EG-Datenschutzrichtlinie** hätte bis zum 24. Oktober 1998 in Bundes- und in Landesrecht umgesetzt werden müssen. Da diese Umsetzung leider weder in den allgemeinen noch in den bereichsspezifischen datenschutzrechtlichen Vorschriften fristgerecht erfolgt ist, setzt sich die Bundesrepublik Deutschland der Gefahr eines Vertragsverletzungsverfahrens aus.

Damit stellt sich nun auch die Frage einer **unmittelbaren Wirkung** der Bestimmungen der EG-Datenschutzrichtlinie. Eine solche direkte Anwendung ist nach der Rechtsprechung des Europäi-

schen Gerichtshofs für nicht fristgerecht in das Recht eines Mitgliedsstaats umgesetzte Vorschriften anzunehmen, die unbedingt und hinreichend genau formuliert sind. Zu denken ist hier an die Vorschriften über das Informations- und das Auskunftsrecht des Betroffenen.

2.2.1 Novellierung des BDSG

Bis zur Bundestagswahl lagen ein in den Ressorts abgestimmter Referentenentwurf der Bundesregierung und ein Entwurf der Fraktion Bündnis 90/Die Grünen zur Novellierung des Bundesdatenschutzgesetzes (BDSG) vor, die jedoch nicht mehr weiterbehandelt wurden.

Inhaltlich halte ich den Entwurf der damaligen Bundesregierung für sehr schwer lesbar und wenig innovativ; mit diesem Entwurf wurde an der bisherigen Konzeption des Bundesdatenschutzgesetzes festgehalten. Zahlreiche Einfügungen und Querverweise erschwerten außerdem die Verständlichkeit und führten dazu, daß dem interessierten Bürger die Materie des Datenschutzrechts kaum vermittelt werden kann. Die in einer Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 ([Anlage 10](#) zu diesem Tätigkeitsbericht) geforderten **Grundsatzentscheidungen** und Anpassungen der Regelungen an die weiterentwickelte Informationsgesellschaft waren nicht enthalten. Zu diesen Grundsatzentscheidungen zähle ich die weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs, die Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen und die Gewährleistung eines einheitlich hohen Datenschutzniveaus durch die Beibehaltung der Funktion des BDSG (und der Landesdatenschutzgesetze) als Querschnittsgesetze. Auch in der Entschließung der 56. Konferenz der Datenschutzbeauftragten vom 05./06.10.1998 ([Anlage 17](#) zu diesem Tätigkeitsbericht) kommen diese und weitere Forderungen (z.B. Stärkung der Rechte der Bürger, Datenschutz durch Technik, Sicherstellung vertraulicher und unverfälschter Kommunikation durch staatliche Förderung von Verschlüsselungsverfahren) zum Ausdruck. Weiterhin vermißte ich eine ausdrückliche Aufnahme des **Grundrechtscharakters** des Datenschutzrechts (Recht auf informationelle Selbstbestimmung) und von wichtigen Grundsätzen, wie z.B. der **Datensparsamkeit**, der **Anonymisierung**, der **Pseudonymisierung**, der **Verschlüsselung** und der **Risikoanalyse**. Ferner fehlen überfällige Regelungen, etwa für **Chipkartenanwendungen** und für die Zulässigkeit von **Videoüberwachungen**.

Der Gesetzentwurf der Fraktion Bündnis 90/Die Grünen enthält dagegen viele dieser notwendigen Grundsatzentscheidungen und innovativen Elemente, wie z.B. die Festschreibung des Grundrechtscharakters, die Möglichkeit eines Datenschutz-Audits, eine Regelung der Videoüberwachung und von Chipkartenanwendungen.

2.2.2 Novellierung des BayDSG

Auch das Bayerische Datenschutzgesetz (BayDSG) wurde nicht fristgerecht novelliert. Wie ich bereits in meinem 17. Tätigkeitsbericht ([Nr. 2.1](#)) zum Ausdruck gebracht habe, besteht nach wie vor eine Handlungspflicht für den bayerischen Gesetzgeber, unabhängig davon, ob und wann der Bund das BDSG novelliert. Das Bayerische Staatsministerium des Innern hatte sich zunächst auf den Standpunkt gestellt, ein Abwarten sei wegen "des Gleichlaufs der Gesetze" erforderlich. Ich stimme mit dem Innenministerium zwar darin überein, daß das BayDSG nicht - zu sehr - vom BDSG abweichen sollte. Dieser Gesichtspunkt tritt jedoch dahinter zurück, daß das EG-Recht ausdrücklich eine fristgerechte Umsetzung der EG-Datenschutzrichtlinie fordert und eine solche auch dringend notwendig ist. Inzwischen höre ich, daß mit Vorrang der Entwurf eines neuen Bayerischen Datenschutzgesetzes vorbereitet werden soll.

Bei der Novellierung des BayDSG werde ich darauf dringen, daß die oben angesprochenen innovativen Elemente auch in dieses Gesetz Eingang finden werden. Daneben werde ich noch weitere Änderungen anregen, die ich im folgenden - ohne Anspruch auf Vollständigkeit - aufführe:

- Die bloße **Anlaßkontrolle bei nur in Akten verarbeiteten Daten** ([Art. 30 Abs. 1 Satz 2 BayDSG](#)) sollte beseitigt werden, da es für diese Beschneidung meiner Prüfungscompetenz keinen sachlichen Grund gibt. Insbesondere bei verdeckten Maßnahmen ist der Betroffene, der von der Maßnahme nichts bemerkt, schutzlos. Der effektive Schutz seiner Grundrechte kann nur durch eine anlaßunabhängige Kontrolle durch den Datenschutzbeauftragten sichergestellt werden. Ich verweise auch auf meine obigen Ausführungen unter [Nr. 1.5](#) und speziell auf nachstehende [Nr. 6.2.7.2](#).
- Ferner sollte der Aufschub meiner **Prüfungskompetenz bei der Datenerhebung in Ermittlungsverfahren** bis nach Abschluß des Strafverfahrens ([Art. 30 Abs. 4 BayDSG](#)) gestrichen werden. Es gibt keine Anhaltspunkte dafür, daß die Strafrechtspflege durch eine

umfassende Kontrollkompetenz behindert würde. Daher gibt es auch in keinem anderen deutschen Land eine vergleichbare Vorschrift. Ferner ist es für die Betroffenen in vielen Fällen unzumutbar, das Ende des Strafverfahrens abzuwarten, bevor Erhebungsmaßnahmen auch einer datenschutzrechtlichen Kontrolle zugeführt werden können.

- Ich werde weiterhin fordern, daß zumindest grundsätzlich für alle bayerischen öffentlichen Stellen die **Berufung interner Datenschutzbeauftragter** gesetzlich vorgeschrieben wird (vgl. bereits in meinem 17. Tätigkeitsbericht, [Nr. 2.1](#)). Dies hätte u.a. den Vorteil, daß unter dieser Voraussetzung Ausnahmen von der in der EG-Datenschutzrichtlinie an sich vorgeschriebenen Meldepflicht oder Vereinfachungen der Meldungen vorgesehen werden können.

2.3 Datenschutz und Forschung

Im zurückliegenden Berichtszeitraum habe ich mein besonderes Augenmerk auf das Verhältnis des Datenschutzrechts zur wissenschaftlichen Forschung gelegt. In einer Denkschrift zur Forschungsfreiheit hatte die Deutsche Forschungsgemeinschaft (DFG) aus ihrer Sicht Beeinträchtigungen der Forschung in Deutschland festgestellt. U.a. wurde moniert, daß die Forschung als Folge von Datenschutzregelungen unnötig erschwert und behindert werde. Angesichts der - zum Teil wenig konkreten - Vorwürfe haben die Datenschutzbeauftragten des Bundes und der Länder das Gespräch mit der DFG gesucht. Es wurde vereinbart, daß zunächst datenschutzrechtliche Fragen im Bereich der Epidemiologie (Lehre von der Verteilung von Krankheiten und ihrer Risikofaktoren in der Bevölkerung) eingehender diskutiert werden sollten.

2.3.1 Gespräche mit der Deutschen Arbeitsgemeinschaft für Epidemiologie

Zu den datenschutzrechtlichen Problemen im Bereich der Epidemiologie legte die Deutsche Arbeitsgemeinschaft für Epidemiologie ein Arbeitspapier vor, das zunächst im Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit einigen Wissenschaftlern besprochen wurde. Ergebnis war ein überarbeitetes Arbeitspapier, das vom Vorstand der Deutschen Arbeitsgemeinschaft für Epidemiologie (DAE) in Abstimmung mit der Deutschen Gesellschaft für medizinische Information, Biometrie und Epidemiologie (GMDS),

der Deutschen Gesellschaft für Sozialmedizin und Prävention (DGSMP), der Deutschen Region der Biometrischen Gesellschaft und von der Konferenz der Datenschutzbeauftragten zustimmend zur Kenntnis genommen wurde.

Danach gibt es folgende rechtliche Rahmenbedingungen für die Forschung mit personenbezogenen Daten:

- Die Forschung mit **anonymisierten** Daten ist jederzeit ohne datenschutzrechtliche Vorgaben möglich. Ob hierbei eine absolute Anonymisierung notwendig ist oder eine faktische Anonymisierung ausreicht, richtet sich nach den jeweiligen (landes-)rechtlichen Bestimmungen.
- Die Verarbeitung personenbezogener Daten wird im Rahmen epidemiologischer Forschung in der Regel auf der Basis einer **Einwilligung** der Betroffenen erfolgen. Erforderlich für die Wirksamkeit einer solchen Einwilligung sind die umfassende Information der Betroffenen über die vorgesehene Datenverarbeitung und in der Regel die Schriftform der Einwilligungserklärung.
- Eine Forschung mit personenbezogenen Daten ohne Einwilligung des Betroffenen ist in einzelnen gesetzlichen Bestimmungen, wie z.B. dem Bayer. Krankenhausgesetz, unter bestimmten Voraussetzungen vorgesehen.
- Eine **Zweckänderung** ist bei der Verarbeitung anonymisierter Daten unproblematisch. Bei der Verarbeitung personenbezogener Daten besteht die Möglichkeit, Einwilligungserklärungen so zu formulieren, daß eine eventuelle inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfaßt ist. Andererseits muß die Einwilligungserklärung jedoch hinreichend bestimmt sein. Ob der Betroffene eine solche Erklärung unterschreibt, ist eine Frage der Akzeptanz des Vorhabens. In Betracht kommt darüber hinaus auch eine Anwendung der datenschutzrechtlichen Regelungen über die Zweckänderung personenbezogener Daten.

2.3.2 7. Wiesbadener Forum Datenschutz

Ebenfalls das Thema Datenschutz und Forschung griff das **7. Wiesbadener Forum Datenschutz** am 18. Juni 1998 auf. Von den verschiedenen Referenten wurden einzelne Problemfelder des Verhältnisses Datenschutz und Forschung beleuchtet. Ich habe mich mit einem Referat zu "Datenschutz und Forschungsfreiheit - Widerspruch oder Weg zur mehrseitigen Grundrechtsrealisierung?" an dem Forum beteiligt. Dabei habe ich ausgeführt, daß zwei Grundrechte nebeneinanderstehen: Zum einen das **Grundrecht auf Wissenschaftsfreiheit** und zum anderen das **Grundrecht auf informationelle Selbstbestimmung**. Beide Grundrechte sind mit dem Ziel einer gegenseitigen Optimierung (praktische Konkordanz) zu realisieren. Beide Rechte begrenzen sich jedoch, so daß sie auch Einschränkungen hinnehmen müssen. Im einzelnen habe ich folgende Forderungen aufgestellt:

- Wie bereits in meinem 16. Tätigkeitsbericht ([Nr. 2.1.1](#)) habe ich erneut die Einführung eines **Forschungsgeheimnisses** befürwortet, mit dem die Strafbarkeit der unbefugten Weitergabe, der Beschlagnahmeschutz und das Zeugnisverweigerungsrecht des Forschers erreicht werden können. Ich teile nicht die gelegentlich vertretene Auffassung, daß der Schutz medizinischer Daten im Bereich der Forschung bereits jetzt ausreichend gewährleistet sei. Forschung wird zum einen auch von Nichtärzten betrieben; aber auch wenn sie von Ärzten betrieben wird, ist keinesfalls sichergestellt, daß der forschende Arzt mit dem behandelnden Arzt im Sinne des § 203 StGB gleichzusetzen ist.
- Die Einführung eines Forschungsgeheimnisses darf jedoch **nicht** zu einem allgemeinen Verzicht auf die **Einwilligung** in die Verwendung der Patientendaten führen. Ein derartiger Verzicht würde den Patienten entmündigen und ihn zum bloßen Forschungsobjekt machen. Das Forschungsgeheimnis könnte aber sowohl die Abwägung im Einzelfall wesentlich erleichtern als auch die Entscheidung des Gesetzgebers, in weiteren Einzelfällen die Verwendung personenbezogener Daten in der Forschung in Grenzen - z.B. wenn die vorherige Einholung der Einwilligung das Forschungsprojekt nachteilig beeinflusst - auch ohne Einwilligung des Betroffenen zu gestatten.

- Darüber hinaus habe ich angeregt, ob die gesetzlichen Vorschriften, die ein **erhebliches Überwiegen** des Forschungsinteresses über das Interesse des Einzelnen vorsehen, dahingehend geändert werden könnten, daß ein (bloß) überwiegendes Forschungsinteresse ausreichend ist. Jedenfalls ist das Tatbestandsmerkmal "erheblich" im Hinblick auf das Grundrecht der Forschungsfreiheit m.E. restriktiv auszulegen, so daß darüber nachgedacht werden sollte, ob nicht ein über den bloßen zusätzlichen Erkenntnisgewinn hinausgehendes überwiegendes Forschungsinteresse als ausreichend angesehen werden muß. Das neue Hessische Datenschutzgesetz enthält in diesem Sinn das Tatbestandsmerkmal "erheblich" nicht mehr.

3. Gesundheitswesen

3.1 Medizinische Forschung und Datenschutz

Auch in diesem Berichtszeitraum habe ich wiederholt bei medizinischen Forschungsvorhaben datenschutzrechtlich beraten. Mir ging es dabei nicht darum, ein konkretes Projekt zu verzögern oder gar zu verhindern, sondern um die Herstellung des notwendigen Ausgleichs zwischen den konkurrierenden Rechten der Patienten und der Forschenden (vgl. hierzu bereits [Nr. 2.3](#) dieses Tätigkeitsberichts). Ich konnte feststellen, daß das notwendige datenschutzrechtliche Problembewußtsein auf Seiten der Wissenschaft in der Regel bereits vorhanden ist und die Forschungsvorhaben häufig nur in einzelnen Punkten aus datenschutzrechtlichen Gründen einer Präzisierung oder Modifizierung bedürfen. Dabei sollte die Wissenschaft berücksichtigen, daß eine einwandfreie datenschutzrechtliche Ausgestaltung einer Studie wesentlich zur Akzeptanz bei den Beteiligten und in der Öffentlichkeit beiträgt. Im Sinne einer positiven Zusammenarbeit zwischen Forschung und Datenschutz hoffe ich, daß forschende Stellen auch in Zukunft rechtzeitig zur Beratung an mich herantreten.

Im einzelnen war bzw. bin ich unter anderem mit folgenden Forschungsprojekten beschäftigt:

3.1.1 Neuordnung des Neugeborenen-Screenings in Bayern

Ein besonders wichtiges Vorhaben, das ich auch wegen seiner bundesweiten Vorreiterstellung intensiv begleite, ist die Neuordnung des Neugeborenen-Screenings in Bayern.

Beim Neugeborenen-Screening wird in einer Früherkennungsuntersuchung in den ersten Lebensstagen von Neugeborenen deren Blut auf angeborene Stoffwechselerkrankungen untersucht ("**Screening**"). Diese - sehr seltenen - Erkrankungen können, frühzeitig erkannt, i.d.R. erfolgreich behandelt werden, z.B. mit einer speziellen Diät. Wird eine geeignete Behandlung versäumt, können die Stoffwechselstörungen zu schweren geistigen und körperlichen Behinderungen oder sogar zum Tod des Kindes führen. Die Kosten einer lebenslangen Behandlung geschädigter Kinder können enorme Höhen erreichen.

Um künftig besser als bisher sämtliche Säuglinge erreichen zu können, wird in einem Modellversuch in Bayern ein neuartiges Kontrollverfahren ("**Tracking**") eingeführt, mit dem festgestellt werden soll, welche Kinder noch nicht untersucht wurden und mit dem gleichzeitig die rechtzeitige "Nachsorge" sichergestellt werden soll. Dieses Tracking wird durch einen Datenabgleich bei den jeweils zuständigen Gesundheitsämtern gewährleistet, die Namen, Wohnort und Geburtsdatum der Neugeborenen mit den Datensätzen der Einwohnermeldeämter vergleichen. Die Koordination des Verfahrens und die in Einzelfällen notwendige Beratung der Beteiligten soll ein noch zu errichtendes "**Screening-Zentrum**" des öffentlichen Gesundheitsdienstes bei dem Landesuntersuchungsamt für das Gesundheitswesen Südbayern gewährleisten.

Ich habe die Durchführung dieser Untersuchung ausdrücklich begrüßt, gleichzeitig aber auf eine datenschutzgerechte Ausgestaltung des Verfahrens gedrungen. Als besonders wichtig sind mir dabei folgende Punkte erschienen:

- Ich habe klargestellt, daß es eine normative Rechtsgrundlage für die Einrichtung des Screening-Zentrums des öffentlichen Gesundheitsdienstes und vor allem für das Tracking nicht gibt. Voraussetzung der angestrebten Datenerhebungen und -verarbeitungen ist damit eine **informierte Einwilligung** des/der Erziehungsberechtigten, die deren vorherige

umfassende Aufklärung notwendig macht. Diese Einwilligung hat gem. [Art. 15 Abs. 3 Satz 1 BayDSG](#) schriftlich zu erfolgen. Besondere Bedeutung kommt daher dem Informationsblatt zu diesem Verfahren zu, an dessen Ausgestaltung ich mitgewirkt habe.

- Weiterhin ist inzwischen gewährleistet, daß die Erziehungsberechtigten in ihrer Wahlmöglichkeit nicht beschränkt sind. Sie können das Kind an der Untersuchung und an dem Tracking-Verfahren, nur an der Untersuchung oder weder an der Untersuchung noch am Trackingverfahren teilnehmen lassen.
- Gegen die Einrichtung eines **zentralen Screening-Zentrums des öffentlichen Gesundheitsdienstes** für ganz Bayern beim Landesuntersuchungsamt für das Gesundheitswesen Südbayern habe ich angesichts der von medizinischer Seite vorgetragenen Argumente aus datenschutzrechtlicher Sicht keine durchgreifenden Bedenken. Bei der geringen Anzahl der tatsächlich zu behandelnden Kinder ist eine zentrale Sammlung der Daten erforderlich, da nur so ein Überblick über ganz Bayern und die angestrebte Qualitätssicherung möglich sein werden. Eine gute Qualität der Auswertung und eine qualifizierte Beratung durch Spezialisten ist nur durch die Beteiligung einer zentralen öffentlichen Stelle gewährleistet.
- Nach dem ursprünglichen Konzept sollten alle den Säuglingen entnommenen Blutproben beim Screening-Zentrum aufbewahrt werden. Dies hätte dazu geführt, daß ab Beginn des Projekts eine Sammlung von Blutproben entstanden wäre, die nahezu die gesamten Geburtsjahrgänge erfaßt hätte. Diese Sammlung hätte als "**Gendatei**" genutzt werden können. Das Verfahren wurde nunmehr so ausgestaltet, daß das untersuchende Labor bei einem negativen Befund die Testkarten und die Blutproben trennt; das betrifft die ganz überwiegende Mehrzahl der Proben (über 99 %). Die Blutproben werden an das Screening-Zentrum gesandt, das diese (jetzt anonymen) Proben für Forschungsvorhaben verwendet. Eine Wiederzusammenführung von Proben und identifizierenden Merkmalen ist nicht möglich. Ich habe dieses Verfahren für zwingend erforderlich gehalten, damit keine umfassende Gendatei bei einer öffentlichen Stelle entsteht.

3.1.2 Sonstige Forschungsvorhaben

An der datenschutzrechtlichen Ausgestaltung folgender wissenschaftlicher Vorhaben habe ich u.a. ebenfalls mitgewirkt. Diese Studien zeigen, daß eine datenschutzgerechte Lösung gefunden werden kann, ohne den Erfolg des konkreten Vorhabens zu beeinträchtigen.

- Das Institut für soziale Pädiatrie und Jugendmedizin der Ludwig-Maximilians-Universität München (LMU) führte eine Untersuchung über das **Auftreten von Übergewicht bei Schulanfängern** in den letzten 20 Jahren in verschiedenen Regionen Bayerns durch. Hierzu wurden in einigen Gesundheitsämtern die Daten der Einschulungsuntersuchungen ausgewertet. Die Namen der Schüler waren für diese Studie nicht von Interesse.

Da eine Rechtsgrundlage zur Datenübermittlung von den Gesundheitsämtern an die LMU nicht besteht und eine vorherige Anonymisierung der Daten durch Mitarbeiter der Gesundheitsämter für diese aus Kapazitätsgründen nicht durchführbar war, habe ich einen anderen Weg vorgeschlagen. Die Datenerhebung erfolgte gem. [Art. 6 BayDSG im Auftrag der Gesundheitsämter](#) durch Mitarbeiter des Instituts der LMU.

Der Schutz und die Förderung der Gesundheit von Menschen ist nach dem bayerischen Gesundheitsdienstgesetz Aufgabe des öffentlichen Gesundheitsdienstes, d.h. auch der Gesundheitsämter. Datenschutzrechtlich verantwortlich bleibt das Gesundheitsamt. Die an die Gesundheitsämter entsandten Mitarbeiter der LMU wurden bei ihrer Tätigkeit durch einen Mitarbeiter des Gesundheitsamts kontrolliert, der die Einhaltung der datenschutzrechtlichen Anforderungen überwachte und dafür sorgte, daß nur die vorgegebenen Daten übernommen wurden.

- In einer weiteren Studie der LMU soll die Möglichkeit einer **Erhöhung der Masern-, Mumps- und Röteln-Impfquote** bei Schulanfängern erforscht werden. Hierzu werden zunächst bei einem einzuschulenden Jahrgang in vier Landkreisen die Impfquoten ermittelt. Danach werden in drei Landkreisen Informationsmaßnahmen durchgeführt: Ein Landkreis legt Informationsmaterial der Bundeszentrale für gesundheitliche Aufklärung aus, im zweiten Landkreis werden (Kinder-)Ärzte informiert und im dritten Landkreis er-

folgt eine telefonische Information/Beratung der Eltern durch Mitarbeiter des Instituts ("telefonische Intervention"). Der vierte Landkreis bleibt zum Vergleich ohne spezielle Information. In der nächsten Phase werden dann die Impfquoten der Schulanfänger des nächsten Jahrgangs ermittelt.

Für mich war vor allem eine datenschutzgerechte Ausgestaltung der telefonischen Intervention wichtig. Zu den Anforderungen an die Gesundheitsdatenerhebung durch Telefonumfragen weise ich auf meinen 17. Tätigkeitsbericht ([Nr. 3.3.3](#)) hin. Ich habe darauf hingewirkt, daß die Erziehungsberechtigten der einzuschulenden Kinder in einem angemessenen Zeitraum vor dem Anruf schriftlich über den Sinn und Zweck der Studie ([Art. 16 Abs. 3 Satz 1 BayDSG](#)), den Umfang der Daten, deren Löschung und die Freiwilligkeit der Teilnahme informiert werden. Ein solcher Hinweis hat nochmals zu Beginn des Telefongesprächs bei der telefonischen Intervention zu erfolgen.

- Eine Forschungseinrichtung wollte für das Projekt "Kooperative Gesundheitsforschung in der Region Augsburg (KORA)" Adreßdaten eines bereits früher durchgeführten Projekts verwenden. Hierzu sollten die Teilnehmer der früheren Studie von den damals beauftragten Befragungsinstituten mit der Bitte, sich zur Durchführung des Projekts bei einem hierfür eingerichteten ärztlichen Untersuchungszentrum zu melden, kontaktiert werden. Den Teilnehmern oblag es dann, von sich aus an die Forschungseinrichtung heranzutreten.

Dieses Verfahren der **Adreßmittlung** begegnet aus datenschutzrechtlicher Sicht keinen Bedenken:

- Eine Weitergabe von Anschriftenmaterial an Dritte erfolgt nicht. Angeschrieben wird lediglich der Betroffene und zwar von der Stelle, die rechtmäßig über seinen Namen und seine Anschrift verfügt.
- Es ist allein Sache des Betroffenen, ob er sich aufgrund des Anschreibens zur Durchführung des neuen Projekts meldet oder nicht.

3.2 Approbation von Psychologen nach dem Psychotherapeutengesetz

Am 16. Juni 1998 beschloß der Deutsche Bundestag mit Zustimmung des Bundesrates das Gesetz über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendpsychotherapeuten (Psychotherapeutengesetz - PsychThG). Dieses Gesetz regelt u.a. die Ausbildung zum Psychotherapeuten und enthält eine Übergangsregelung, nach der Psychologen, die bisher bereits psychotherapeutisch tätig waren, unter bestimmten Voraussetzungen die Approbation zum Psychotherapeuten erhalten können. Zu diesen Voraussetzungen gehört u.a. eine festgelegte Anzahl von Behandlungsstunden oder Behandlungsfällen, die der Antragsteller in einem bestimmten Zeitraum durchgeführt hat.

Das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit als zuständige Approbationsbehörde entwickelte zum Nachweis der Behandlungen ein Verfahren, das anonymisierte Bestätigungen der gesetzlichen Krankenkassen, der privaten Krankenversicherungen und der Beihilfestellen vorsieht. Diese Nachweise mit nicht personenbezogenen Daten begrüße ich aus datenschutzrechtlicher Sicht.

Dagegen sollten ursprünglich die Psychologen in den Fällen, in denen diese anonymen Nachweise nicht vorgelegt werden können, fallbezogene Kurzdokumentationen unter Angabe des Patientennamens vorlegen. Dies wäre z.B. der Fall gewesen, wenn eine Versicherung die notwendige Bestätigung nicht ausstellen kann oder will sowie bei den Selbstzahlern, die nicht über die o.g. Kostenträger abgerechnet hatten. Das Staatsministerium begründete den personenbezogenen Nachweis mit der Gefahr von Täuschungsversuchen.

Ich habe darauf hingewiesen, daß ich diese Vorgehensweise für datenschutzrechtlich unzulässig halte. Ein Psychologe unterliegt der Schweigepflicht gemäß § 203 Abs. 1 Nr. 2 StGB. Zur Offenbarung ihm anvertrauter Geheimnisse bedarf er einer Offenbarungsbefugnis, wie sie z.B. die ausdrückliche Einwilligung eines Patienten darstellt. Das Psychotherapeutengesetz enthält keine Offenbarungsbefugnisse. Ich habe dem Ministerium eine **Anonymisierung** der vorzulegenden Unterlagen durch eine **Schwärzung personenbezogener Merkmale** vorgeschlagen und zum Ausdruck gebracht, daß nur im Falle des konkreten Verdachts eines Täuschungsversuchs ausnahmsweise nicht anonymisierte Belege verlangt werden können, soweit dies für die

Überprüfung erforderlich sei.

Der Arbeitskreis "Gesundheit und Soziales" der Datenschutzbeauftragten des Bundes und der Länder, dessen Vorsitz ich inne habe, beschäftigte sich in seiner 30. Sitzung am 10./11. September 1998 mit dieser Problematik. Dabei wurden die Gesundheitsministerien aufgefordert, ein datenschutzgerechtes Verfahren zu entwickeln, das die Nachweise unter Wahrung der Schweigepflicht ermöglicht. Die Nachweispflichtigen könnten jedoch verpflichtet werden, die personenbezogenen Unterlagen für einen bestimmten Zeitraum vorzuhalten. Sofern sich im Einzelfall bei der Prüfung der vorgelegten Nachweise Anhaltspunkte für falsche Darstellungen ergeben, dürften die Angaben der Nachweispflichtigen überprüft werden. Die Nachweispflichtigen dürften dann personenbezogene Daten unter dem Gesichtspunkt der Wahrnehmung berechtigter Interessen offenbaren.

Das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit, wie auch - soweit bekannt - die zuständigen Ministerien der anderen Länder, hat diesen Forderungen Rechnung getragen und in den Regelungen zum Nachweisverfahren eine Anonymisierung der personenbezogenen Patientendaten vorgesehen; danach darf z.B. nur noch der jeweils erste Buchstabe des Vor- und Nachnamens des Patienten erkennbar sein.

3.3 Datenschutzfragen aus dem Bereich von Krankenhäusern 3.3.1 Einzelfragen aus der Prüfung und Beratung

Bei der Prüfung von Krankenhäusern und bei Anfragen zum Datenschutz in Krankenhäusern stelle ich immer wieder fest, daß in bestimmten Punkten noch datenschutzrechtliche Verbesserungen notwendig sind, auf die ich zum Teil bereits in früheren Tätigkeitsberichten hingewiesen habe:

- Zur Bestellung eines **Datenschutzbeauftragten in öffentlichen Krankenhäusern** habe ich mich bereits in meinem 16. Tätigkeitsbericht ([Nr. 2.3.5](#)) geäußert. Es stellte sich nunmehr die Frage, ob die Bestellung des **stellvertretenden Verwaltungsleiters** eines Krankenhauses zum Datenschutzbeauftragten zulässig ist. Er ist zwar nicht kraft Gesetzes von dieser Tätigkeit ausgeschlossen; eine Bestellung sollte jedoch gleichwohl ausscheiden, da bei ansonsten gleichbleibender Aufgabenzuweisung die Gefahr einer Interessen-

kollision besteht. Da der Datenschutzbeauftragte der datenschutzrechtlichen Eigenkontrolle dient und ihm Beratungsfunktionen gegenüber dem Leiter der Einrichtung zugewiesen sind, ist zumindest im Vertretungsfall eine solche Interessenkollision sehr wahrscheinlich.

- Immer wieder muß ich feststellen, daß die Krankenhäuser zu viele Daten von ihren Patienten erheben. Das liegt auch daran, daß die Datenerhebung i.d.R. von dem verwendeten **Krankenhausinformationssystem** vorgegeben wird. Hierzu weise ich auf Art. 27 Abs. 2 Satz 1 BayKrG hin, wonach Patientendaten nur erhoben und aufbewahrt werden dürfen, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausesärztlichen Behandlungsverhältnisses erforderlich ist oder die betroffene Person eingewilligt hat. Dabei ist zu berücksichtigen, daß auch bei Einwilligung des Patienten nicht mehr Daten erhoben werden dürfen, als für die Aufgabenerfüllung des Krankenhauses erforderlich ist. Diese rechtlichen Vorgaben des Bayerischen Krankenhausgesetzes sind bei der Datenerhebung zu beachten und ggf. gegenüber dem Vertreiber eines Krankenhausinformationssystems geltend zu machen. Im einzelnen ist mir u.a. folgendes aufgefallen:

Lediglich dort, wo für bestimmte Konfessionen eine Krankenhauseelsorge angeboten wird, halte ich es für zulässig, diese konkreten Religionszugehörigkeiten der Patienten zu erfragen. Die Erhebung dieser **Religionszugehörigkeiten** ist allerdings mit einem Hinweis auf den Grund und die Freiwilligkeit der Angabe zu verbinden. Gibt ein Patient seine Religionszugehörigkeit freiwillig an, so halte ich es auch bei fehlender ausdrücklicher Befragung für datenschutzrechtlich zulässig anzunehmen, daß er mit der Verständigung des für ihn zuständigen Krankenhauseelsorgers einverstanden ist, weil er mit einer solchen rechnen muß. Die Mitteilung der Privatadressen und Geburtsdaten der Patienten an den jeweiligen Seelsorger halte ich nicht für notwendig. Die Weitergabe der Daten an die jeweilige Heimatgemeinde bzw. an einen Laienbesuchsdienst der Heimatgemeinde ist datenschutzrechtlich nur zulässig, wenn der Patient dieser Datenweitergabe ausdrücklich zugestimmt hat.

Beim **Familienstand** ist nur die Erhebung des Datums "verheiratet" erforderlich. Wird diese Frage mit nein beantwortet, sind weitere Differenzierungen nicht notwendig.

- Wie ich bereits in meinem 15. Tätigkeitsbericht (Nr. 2.1) ausgeführt habe, werden von vielen Krankenhäusern zu viele Daten an die **gesetzlichen Krankenkassen** übermittelt. Dies liegt daran, daß häufig sämtliche bei der Aufnahme erhobenen Daten an die Krankenkassen weitergegeben werden. Zulässig ist jedoch nur die Übermittlung der im Katalog des § 301 Abs. 1 (i.V.m. § 291 Abs. 2 Nr. 1 bis 8) SGB V festgelegten Daten. Die darüber hinausgehenden Daten (z.B. Beruf, Arbeitgeber, Konfession, Familienstand) sind in der Aufnahmeanzeige gegenüber den gesetzlichen Krankenkassen wegzulassen.
- Weiterhin weise ich erneut darauf hin, daß [Art. 26 BayDSG](#) (datenschutzrechtliche Freigabe) verlangt, daß auch Krankenhäuser vor dem erstmaligen Einsatz automatisierter Verfahren ein **Freigabeverfahren** durchzuführen haben. Außerdem müssen **Anlagen- und Verfahrensverzeichnisse** erstellt werden, die den Anforderungen des [Art. 27 BayDSG](#) genügen. Stellen, die diesen Verpflichtungen nicht nachkommen, müssen bei einer datenschutzrechtlichen Prüfung mit einer Beanstandung rechnen.
- Ferner weise ich darauf hin, daß gem. [Art. 26 Abs. 2 Nr. 7 BayDSG](#) die datenschutzrechtliche **Freigabe automatisierter Verfahren** Angaben zu den verarbeitungs- und nutzungsberechtigten Personengruppen enthalten muß. Diese Angaben sind gem. [Art. 27 Abs. 2 BayDSG](#) auch in das Anlagen- und Verfahrensverzeichnis aufzunehmen. Wegen der besonderen datenschutzrechtlichen Bedeutung der Zugriffsberechtigungen in den Krankenhausinformationssystemen halte ich ein differenziertes **Berechtigungskonzept** für unbedingt notwendig (siehe hierzu im einzelnen [Nr. 3.3.2](#) dieses Tätigkeitsberichts).

3.3.2 Ausgestaltung der Zugriffsberechtigungen in Krankenhausinformationssystemen

Immer wieder erhalte ich Anfragen von Ärzten und Krankenhäusern, auf welche Patientendaten Ärzte oder andere Mitarbeiter von Krankenhäusern Zugriff nehmen dürfen. Diese Frage spielt mit der zunehmenden Verbreitung von DV-Systemen in Krankenhäusern eine immer wichtigere Rolle (vgl. auch [Nr. 3.3.3](#)).

Zunächst ist festzuhalten, daß die Einführung und technische Weiterentwicklung von Krankenhausinformationssystemen an den rechtlichen Grundlagen der Datenverarbeitung im Krankenhaus nichts ändert. Dies bedeutet, daß sich auch die Ausgestaltung der DV in Krankenhäusern an den bestehenden gesetzlichen Vorschriften auszurichten hat. Zu diesen gehört insbesondere die **ärztliche Schweigepflicht** im Sinne des § 203 Abs. 1 StGB, wonach sich ein Arzt strafbar macht, wenn er unbefugt ein fremdes Geheimnis offenbart, das ihm als Arzt anvertraut oder sonst bekanntgeworden ist. Es kann nicht oft genug betont werden, daß diese Schweigepflicht auch gegenüber anderen Ärzten außerhalb, aber auch innerhalb eines Krankenhauses gilt. Offenbarungsbefugnisse im Sinne dieser Vorschrift enthält insbesondere Art. 27 Abs. 4 des Bayerischen Krankenhausgesetzes. Gemäß Art. 27 Abs. 4 Satz 1 BayKrG dürfen Krankenhausärzte Patientendaten nutzen, soweit dies im Rahmen des krankenhausesärztlichen Behandlungsverhältnisses, zur Aus-, Fort- und Weiterbildung im Krankenhaus, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Absatz 4 Satz 2 dieser Vorschrift bestimmt u.a., daß sie damit andere Personen im Krankenhaus beauftragen können, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Grundlage für die Zulässigkeit des Zugriffs von Krankenhausärzten und anderem Personal auf Patientendaten ist also immer die **Erforderlichkeit** des konkreten Zugriffs.

Diese rechtlichen Vorgaben zum Schutz der Patienten, deren sensible Daten nicht vom ganzen Krankenhaus zur Kenntnis genommen werden dürfen, sind in einem **Berechtigungskonzept** umzusetzen. Auch die datenschutzrechtliche Freigabe automatisierter Verfahren hat gem. [Art. 26 Abs. 2 Nr. 7 BayDSG](#) ein solches Konzept zu enthalten. Es

muß einerseits die rechtlichen Vorgaben möglichst exakt abbilden, darf andererseits jedoch nicht so starr sein, daß ein erforderlicher Zugriff, z.B. in Notfällen, nicht möglich ist.

Die Ausgestaltung von Zugriffsberechtigungen wurde mehrmals im Arbeitskreis "Gesundheit und Soziales" der Datenschutzbeauftragten des Bundes und der Länder diskutiert und wird in Zukunft in meiner Beratungs- und Prüfungstätigkeit eine große Rolle spielen. Ich kann zwar keine endgültige Lösung für alle relevanten Fragestellungen anbieten, die Ausgestaltung der Krankenhausinformationssysteme sollte sich jedoch an folgenden Leitlinien orientieren (vgl. hierzu auch zu den Sicherheitsmaßnahmen in technischer Hinsicht [Nr. 19.3.4](#) dieses Tätigkeitsberichts):

- Eine **Zugriffsberechtigung aller Abteilungen** eines Krankenhauses auf alle patientenbezogenen Daten ist nicht erforderlich. Hiervon ist die Zugriffsmöglichkeit auf den **Stammdatensatz** (Name, Adresse, Geburtsdatum etc.) eines Patienten zu unterscheiden. Auch ein solcher Zugriff ist jedoch nicht jedem Mitarbeiter der jeweiligen Abteilung zu ermöglichen, sondern auf die zuständige Leitstelle (z.B. das Stationszimmer) zu beschränken.
- Der **behandelnden Fachabteilung** ist grundsätzlich ein Zugriffsrecht auf alle Daten der dortigen Patienten einzuräumen. Eine unbeschränkte Zugriffsmöglichkeit muß für die Ärzte dieser Station bestehen. Dagegen wird in der Regel für Pflegekräfte und sonstige Beschäftigte (z.B. Auszubildende, Studenten, Praktikanten etc.) ein unbeschränkter Zugriff nicht erforderlich sein. Die Zugriffsberechtigung für diese Personengruppen ist auf der Grundlage der Erforderlichkeit für deren Aufgabenerfüllung konkret festzulegen. Wegen der Sachnähe dürfte dafür regelmäßig der Chef der behandelnden Fachabteilung in Betracht kommen.
- Eine **abteilungsübergreifende Zugriffsberechtigung** ist beim Vorliegen eines Behandlungszusammenhangs - ebenfalls im Rahmen der Erforderlichkeit - vorzusehen. Dies ist z.B. der Fall, wenn eine andere Abteilung als die an sich zuständi-

ge den Patienten mit- oder nachbehandelt. In diesem Fall muß die Initiative für die Eröffnung des Zugriffs von der behandelnden Abteilung ausgehen, d.h. sie muß die Daten - im erforderlichen Umfang - für die mit- bzw. nachbehandelnde Abteilung freigeben.

- In Sonderfällen muß ein **abteilungsübergreifender Zugriff** ohne das Vorliegen eines Behandlungszusammenhangs möglich sein, der aber auf das Notwendige zu beschränkt ist. Hier ist z.B. an den Notfalleinsatz, den Nacht- und den Wochenenddienst zu denken. Zu gewährleisten ist die Erforderlichkeit des konkreten Zugriffs durch ein speziell auf diese Tätigkeitsbereiche abgestimmtes Nutzungsprofil der Berechtigten.
- Bei einer erneuten **Einlieferung in eine andere Abteilung** wird diese als behandelnde Fachabteilung in das System eingetragen. Hinsichtlich der Einsichtnahme in die bereits vorhandenen Unterlagen durch die neue Abteilung wird in der Regel die mutmaßliche Einwilligung des Patienten anzunehmen sein, falls dieser einer solchen Einsichtnahme nicht ausdrücklich widerspricht. Davon wird man aber in speziellen Fällen nicht ausgehen können, z.B. dann, wenn ein Patient ursprünglich in der psychiatrischen Abteilung behandelt wurde und später in der orthopädischen Abteilung behandelt wird.
- Der Zugriff auf Patientendaten für bloße **Verwaltungszwecke** hat sich strikt an der Erforderlichkeit für die Aufgabenerfüllung zu orientieren.

Eine reine **Protokollierung** der Zugriffe auf Patientendaten, um nachträglich in strittigen Fällen deren Erforderlichkeit beurteilen zu können, halte ich nicht für ausreichend. Vielmehr ist ein differenziertes Berechtigungskonzept notwendig und im Programm abzubilden, um von vornherein nicht berechtigte Zugriffe möglichst verhindern zu können. Darüber hinaus ist die (teilweise) Protokollierung der Zugriffe eine geeignete Maßnahme, um unberechtigte Zugriffe innerhalb grundsätzlich bestehender Berechtigungen aufzeigen zu können.

3.3.3 Krankenhausinformationssystem in den städtischen Krankenhäusern Münchens

Im Dezember 1996 beschloß der Stadtrat der Landeshauptstadt München die Einführung der Anwendungssoftware SAP R/3 in den städtischen Krankenhäusern. Wie ich dem Erfahrungsaustausch mit anderen Landesbeauftragten für den Datenschutz entnehmen konnte, findet diese - nicht speziell für Krankenhäuser entwickelte - Software auch in anderen Kliniken bundesweit Anwendung. Im einzelnen haben sich bei meinen Prüfungen folgende Problembereiche ergeben:

- Die gem. [Art. 26 Abs. 1 BayDSG](#) **vor** dem erstmaligen Einsatz von automatisierten Verfahren erforderliche datenschutzrechtliche **Freigabe** ist nicht erfolgt. Im Rahmen der Freigabe hat die zuständige Stelle zu prüfen, ob die beabsichtigte Verarbeitung personenbezogener Daten datenschutzrechtlich zulässig ist. Die Freigabe dient also der **Problemlösung vor dem Echteinsatz** eines automatisierten Verfahrens. Abgesehen hiervon könnte eine vor dem Einsatz erfolgte datenschutzrechtliche Freigabe auch kostspielige Änderungen einer Software verhindern helfen, falls sich das Verfahren als mit den datenschutzrechtlichen Bestimmungen unvereinbar erweist.
- Weiterhin wurde es versäumt, bereits **vor** dem Einsatz dieser Software mit Echtdaten wenigstens ein grundsätzliches System von Zugriffsberechtigungen zu entwickeln (vgl. [Art. 26 Abs. 2 Nr. 7](#) i.V.m. [Art. 27 BayDSG](#)). Wie ich mich inzwischen in einem der Krankenhäuser überzeugen konnte, kann ein solches **Berechtigungskonzept** im Rahmen von SAP R/3 durchaus entwickelt werden. Näheres zu seiner Ausgestaltung enthält dieser Tätigkeitsbericht unter [Nr. 3.3.2](#). In künftigen Prüfungen werde ich mein Augenmerk verstärkt auf die Ausgestaltung eines schriftlichen Berechtigungskonzepts und dessen technische Umsetzung legen.
- Neben einem detaillierten Berechtigungskonzept ist zur technisch-organisatorischen Absicherung einer rechtmäßigen Datenverarbeitung die (teilweise) **Protokollierung der Zugriffe** notwendig; sie muß angesichts des damit verbundenen Aufwands in einem angemessenen Verhältnis zum Schutzzweck stehen. Sie ist insbesondere dafür geeignet, feststellen zu können, ob innerhalb der jeweiligen Berechtigungen mißbräuchliche Zugriffe erfolgt sind. Die Protokollierung der Zugriffe macht die vorher dargestellte Erar-

beutung eines Berechtigungskonzepts nicht überflüssig, da die Protokollierung nur nachträglich nicht erforderliche/berechtigte Zugriffe feststellt. Zugriffe nicht Berechtigter kann die Protokollierung alleine nicht verhindern. SAP R/3 führt kein Protokoll, aus dem ersichtlich ist, wer wann lesenden Zugriff genommen hat.

- Ebenfalls problematisch ist die fehlende Möglichkeit der **Löschung** der im System gespeicherten Daten. Eine Löschungsfunktion sieht SAP R/3 insoweit nicht vor. Eine solche ist jedoch vor allem im Hinblick auf die Fälle, in denen das Krankenhaus keine Leistung erbracht hat, erforderlich. Solche Fälle liegen z.B. vor, wenn ein Patient vor Erbringung einer Leistung das Krankenhaus wieder verläßt oder in ein anderes Krankenhaus weitergeleitet wird. Das Überschreiben entsprechender Daten kann nur als Übergangslösung dienen, da die Möglichkeit einer Wiederherstellung besteht. SAP R/3 läßt eine **Sperrung** von Datensätzen ebenfalls nicht zu. Diese ist notwendig, falls ein Patient das Krankenhaus verlassen hat, sowie die Leistungen abgerechnet und bezahlt wurden, da ein Zugriff auf diese Daten dann in der Regel nicht mehr erforderlich ist. Der gesperrte Satz bräuchte erst dann wieder aktiviert werden, wenn der Patient erneut aufgenommen wird.

Auf obige Punkte werde ich künftig bei der Beratung von Krankenhäusern und deren Prüfung besonderes Augenmerk legen. Ggf. müssen die Anwender des Systems auf eine datenschutzgerechte Ausgestaltung durch die Vertreiber der Software hinwirken.

3.3.4 Fremd- und Fernwartung von Datenverarbeitungssystemen im medizinischen Bereich, insbesondere in Krankenhäusern

In der modernen Medizin wird heute eine Vielzahl technischer Geräte eingesetzt, deren alleinige Wartung durch Klinikpersonal wegen der dafür benötigten Spezialkenntnisse vielfach nicht mehr möglich ist. Diese Geräte speichern und verarbeiten zum Teil hoch sensible Patientendaten, die unter dem Schutz der ärztlichen Schweigepflicht stehen. Auf den Rechnern ist meist auch noch Fremdsoftware im Einsatz, so daß bei Störungen sowie bei in der Hard- oder Software auftretenden Fehlern oft der Hersteller eingeschaltet werden muß. Das kann vor Ort geschehen, meist

jedoch im Rahmen des Teleservice, also in Form einer Ferndiagnose und -wartung. Bei der Hardwarewartung wird in der Regel nur auf bestimmte Statusinformationen in eigens dafür eingerichteten Diagnosedateien zugegriffen, die keine personenbezogenen Daten enthalten. Bei vielen DV-Systemen kann aber die Fehlerdiagnose und -behebung mit einer Offenbarung geschützter Patientendaten verbunden sein.

Datenschutzrechtlich besonders problematisch ist die Fernwartung. Bei einer Wartung vor Ort sind die Kontroll- und Eingriffsmöglichkeiten des Krankenhauspersonals im Regelfall größer. Es ist dann für das Krankenhaus eher erkennbar und prüfbar, welche konkreten Personen in Erscheinung treten und ein "Entfernen", Verändern, unzulässiges Lesen oder Übertragen von Daten ist durch die Kontrolle erschwert. Wegen der besonderen Schutzbedürftigkeit der Patientendaten bei der Fernwartung beziehen sich die folgenden Ausführungen vor allem auf diese. Sinngemäß gelten sie jedoch auch für die Fremdwartung vor Ort. Es wäre sehr bedenklich, wenn die Krankenhäuser die Herrschaft über ihre Datenverarbeitung aus Kostengründen vollständig außer Haus gäben.

Abgesehen von der schwierigen datenschutzrechtlichen Einordnung der Fremd- und Fernwartung (vgl. insoweit meinen 14. Tätigkeitsbericht, Nr. 2.2) ist entscheidend, daß es hier zu einer Offenbarung von Patientendaten kommen kann. Da diese Daten der ärztlichen Schweigepflicht gem. § 203 Abs. 1 StGB unterliegen, bedarf die Kenntnisnahme Dritter einer Offenbarungsbefugnis. In meinem 14. Tätigkeitsbericht habe ich die Möglichkeit einer Rechtfertigung unter dem Gesichtspunkt des **mutmaßlichen Einverständnisses** des Patienten offengelassen und vorgeschlagen, die Einwilligung des Patienten über eine Klausel im **Krankenhausaufnahmevertrag** einzuholen.

Im Hinblick auf das Urteil des Oberlandesgerichts Düsseldorf vom 20. August 1996 (vgl. [Nr. 3.3.5.2](#) in diesem Tätigkeitsbericht), wonach eine Archivierung von Patientendaten außerhalb eines Krankenhauses ohne ausdrückliche Einwilligung des Patienten unzulässig ist und von einer mutmaßlichen rechtfertigenden Einwilligung der Patienten nicht die Rede sein kann, und auf die Tatsache, daß die Fernwartung in diesem Punkt durchaus mit der externen Archivierung vergleichbar ist, halte ich zur Minimierung des rechtlichen Risikos der Fernwartung und der

Fremdwartung grundsätzlich die **ausdrückliche Einwilligung** des Patienten im Krankenhausaufnahmevertrag für erforderlich; die entsprechende Klausel wäre im Vertragstext in geeigneter Weise hervorzuheben, wobei sich allerdings die Frage stellt, inwieweit eine solche Einwilligung als freiwillig bezeichnet werden kann, wenn der Patient keine Alternativen hat. Schon deswegen sollte vor allem die Fernwartung stets als letztes Mittel eingesetzt werden. Bei der besonderen Empfindlichkeit der Patientendaten muß auf alle Fälle zur Überwachung der Fern- und Fremdwartung in den Häusern selbst Sachverstand vorhanden sein.

Zur Minimierung der möglichen Kenntnisnahme von Patientendaten ist bei Fremd- und Fernwartung von Datenverarbeitungssystemen die Einhaltung folgender Sicherheitsmaßnahmen zu beachten:

- **Arbeiten am Testsystem**

Soweit wie möglich sollen Externe nur an solchen Systemen arbeiten, in denen entweder nur signifikante Testfälle (ohne Bezug auf eine konkrete Person) oder anonymisierte Patientendaten gespeichert sind.

- **Arbeiten im Produktionssystem**

Ist für eine Fehlerdiagnose und -behebung der Zugriff auf das Produktionssystem erforderlich, sollten folgende Maßnahmen ergriffen werden:

- Verbindungsaufbau

Bei der Fernwartung ist die Verbindung oder die Freischaltung (nach einem Authentifikationsprozeß) stets vom Anwender aus aufzubauen (Call-Back-Verfahren) oder frei zu geben, damit sichergestellt ist, daß keine unbefugten Einwählversuche stattfinden können. Nach Abschluß der Wartungsarbeiten ist diese Verbindung wieder zu deaktivieren.

- Zugriff

Vom Anwender sind der Wartung/Fernwartung nur solche Zugriffsmöglichkeiten zu eröffnen, die für die Fehlerbehebung unbedingt erforderlich sind. Diese Zugriffe sind unter einer extra dafür eingerichteten Kennung mit einem Paßwort, das nur einmal verwendet werden kann, durchzuführen. Es ist ferner darauf zu achten, daß im Rahmen der Wartung bzw. Fernwartung keine Funktionen frei geschaltet werden, die eine Übertragung oder Auswertung von Anwenderdatenbeständen zulassen. Ein zweckwidriger Zugriff auf andere Rechner im Netz ist zu unterbinden.

- Vieraugenprinzip

Alle Aktivitäten der Wartung bzw. Fernwartung muß ein sachverständiger Mitarbeiter des Krankenhauses am Bildschirm verfolgen können. Im Zweifelsfalle muß dieser Mitarbeiter auch diese Aktivitäten abrechnen können. (Bei manchen Systemen ist das nur eingeschränkt möglich, hier müssen stärkere Protokollierungsvorschriften greifen.)

- Protokollierung

In einem Protokoll sind alle Aktivitäten der Wartung bzw. Fernwartung aufzuzeichnen. Bei besonders kritischen Aktionen ist der gesamte Dialog zu protokollieren, damit später erkennbar wird, auf welche Daten zugegriffen wurde. So gibt es beispielsweise Systeme, die eine ganze Sitzung (alle Aktivitäten am Bildschirm) gleichsam wie in einem Video aufzeichnen können.

- Vertraulichkeit auf dem Übertragungswege

Zur Sicherung der Vertraulichkeit der übertragenen Daten auf dem Übertragungswege kann es erforderlich sein, daß die Daten verschlüsselt werden. Es ist in diesem Falle jedoch darauf zu achten, daß die Protokollierung vor Ort unverschlüsselt erfolgt. Nur so ist eine effektive Kontrolle durch den Anwender gewährleistet.

Organisatorische Maßnahmen

Die Wartung und vor allem die Fernwartung sind auf eine vertragliche Grundlage zu stellen, in der das Wartungsunternehmen explizit auf die Wahrung des Patientengeheimnisses verpflichtet wird. Für Zuwiderhandlungen sind empfindliche Vertragsstrafen vorzusehen. Die Unternehmen müssen außerdem Erklärungen über die Zuverlässigkeit für die mit Wartungsarbeiten befaßten Mitarbeiter abgeben; unter Umständen empfiehlt es sich, sogar Sicherheitsüberprüfungen zu verlangen. Zu meiner Forderung nach einem weitergehenden Schutz des Patientengeheimnisses entsprechend dem Arztgeheimnis im Zusammenhang mit der Auslagerung von DV-Arbeiten verweise ich auf [Nr. 3.3.5](#) dieses Tätigkeitsberichts.

Die externen Mitarbeiter müssen der Klinik oder dem Krankenhaus namentlich benannt werden. Dieser Personenkreis soll aber überschaubar bleiben und möglichst wenig wechseln.

Bei lokaler Wartung sind in einem Logbuch Zeitpunkt, Ursache und Name dessen, der die Wartung durchführt, festzuhalten. Schließlich sollte die Wartung und Fernwartung nur dann durchgeführt werden, wenn sichergestellt ist, daß ausreichender eigener Sachverstand für die Beurteilung der externen Aktivitäten vorhanden ist. Für alle Wartungs- und Fernwartungsaktivitäten ist ein Logbuch zu führen. Aus den Einträgen müssen der Grund der Wartung, der Zeitpunkt und die die Wartung durchführende Person sowie die Wartungsaktivitäten, insbesondere ob auf den Echtdatenbestand zugegriffen werden mußte, erkennbar sein.

3.3.5 Outsourcing im Krankenhaus

Gegenüber dem letzten Berichtszeitraum haben sich die Tendenzen zur "Auslagerung" von Tätigkeitsbereichen durch die Krankenhäuser an Externe weiter verstärkt. Infolge des wachsenden Kostendrucks im Gesundheitswesen sind auch die Krankenhäuser zunehmend bestrebt Aufgaben, die traditionell durch eigene Mitarbeiter im Hause erledigt wurden, durch externe Kräfte erledigen zu lassen. Da hier oft das besonders sensible Arzt-Patienten-Verhältnis betroffen ist, dürfen nicht ausschließlich ökonomische Aspekte für eine Vergabe von Tätigkeiten an Außenstehende ausschlaggebend sein. Der Krankenhausträger muß sich jeweils fragen, ob es nicht zum Schutz der Patienten erforderlich ist, gerade diese konkrete Aufgabe im Krankenhaus durch eigene Kräfte zu erledigen.

Um die vielfältigen Aspekte des Outsourcing richtig bewerten zu können, habe ich mich an der Arbeitsgruppe "**Outsourcing von Datenverarbeitungsaufgaben**" der Datenschutzbeauftragten des Bundes und der Länder beteiligt, die sich umfassend mit dieser Problematik - auch außerhalb des Krankenhausbereichs - beschäftigt (vgl. zum Outsourcing von DV-Leistungen in technischer Hinsicht auch [Nr. 19.3.2](#) dieses Tätigkeitsberichts).

Aus der Sicht der Patienten dürfte der wichtigste Gesichtspunkt beim Outsourcing sein, daß der **Schutz der Patientendaten gegen Beschlagnahme** außerhalb der Krankenhäuser in der Regel nicht gewährleistet ist. Solange hier keine entsprechenden gesetzlichen Regelungen existieren, ist besondere Zurückhaltung geboten. Außerdem dürfen die Krankenhäuser nicht wesentliche Bereiche ihrer Datenverarbeitung in die Hände Dritter geben. Damit soll verhindert werden, daß sie sich von diesen abhängig machen. Gerade wegen der besonderen Sensibilität vieler Patientendaten müssen die Krankenhäuser ein gewisses Grund-Know-How im Umgang mit der Datenverarbeitung aufweisen können.

Zum **Schutz medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen** hat sich die 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18.04.1997 mit einer EntschlieÙung geäußert, die im Anhang als [Anlage 8](#) abgedruckt ist. Diese EntschlieÙung schließt mit der Bitte an den Bundesgesetzgeber, für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für deren Weitergabe für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Im folgenden stelle ich zwei Schwerpunkte aus diesem Themenkreis dar, mit denen ich mich im Berichtszeitraum beschäftigt habe.

3.3.5.1 Externe Vergabe von Schreibarbeiten durch Krankenhäuser

Mit dem Problem des externen Schreibens von **Arztbriefen** war ich mehrfach konfrontiert.

Hierbei ist zu bedenken, daß jede Weitergabe von Patientendaten eine **Durchbrechung der ärztlichen Schweigepflicht** darstellt, die einer Rechtfertigung bedarf. Eine solche ergibt sich nicht aus wirtschaftlichen Interessen. Art. 27 Abs. 4 Satz 6 des Bayerischen Krankenhausgesetzes läßt eine Vergabe von Schreibarbeiten nur an andere Krankenhäuser zu, soweit dabei Behandlungsdaten verarbeitet werden. Außerdem besteht der **Beschlagnahmeschutz** für die der ärztlichen Schweigepflicht unterfallenden Patientendaten nach § 97 Abs. 2 StPO bei einer externen Vergabe nicht mehr, da sich die Unterlagen dann nicht mehr im Gewahrsam einer Kranken-

anstalt befinden.

Möglich wäre es zwar grundsätzlich, eine **Einwilligung** jedes einzelnen Patienten zur externen Vergabe der Schreibearbeiten einzuholen. Hierbei ist jedoch folgendes zu beachten:

- Dem Patienten muß die Tragweite seiner Einwilligung klar sein.
- Bei Krankheiten, die in der gesellschaftlichen Anschauung negativ belegt sind (z.B. Geschlechtskrankheiten, HIV-Infektion, psychische Erkrankungen etc.), sollten die hierzu anfallenden Schreibearbeiten in keinem Fall durch externe Kräfte durchgeführt werden.
- Dem Patienten sollten Name und Anschrift des beauftragten Schreibbüros mitgeteilt werden, damit er erkennen kann, ob die Vergabe seine Interessen berührt, z.B. weil Verwandte oder Bekannte dort arbeiten.
- Auch bei Vorliegen einer Einwilligung dürfen Unterlagen nur im unbedingt erforderlichen Umfang an den Externen gegeben werden. So ist es regelmäßig nicht statthaft, den Diktatkassetten auch Behandlungsunterlagen beizufügen.

Selbst bei Vorliegen einer Einwilligung des Patienten ergeben sich jedoch folgende Schlussfolgerungen:

- Die externen Schreibkräfte sollten in den Räumen des Krankenhauses arbeiten, da dadurch der Gewahrsam des Krankenhauses und damit die Beschlagnahmefreiheit der Krankenunterlagen bestehen bleiben.
- Die Schreibkräfte sind nach dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten förmlich zu verpflichten, wodurch sie einem Amtsträger gleichgestellt werden.

Wenn der Patient nicht in die externe Vergabe von Schreibearbeiten einwilligt, sind diese zuverlässig vom Krankenhaus selbst zu erledigen.

3.3.5.2 Externe Archivierung von Krankenunterlagen

Von verschiedener Seite wurde ich um Äußerung gebeten, wie **eine externe Archivierung von Krankenunterlagen** datenschutzrechtlich zu bewerten ist. In meinem 17. Tätigkeitsbericht ([Nr. 3.4.1.5.](#)) habe ich bereits Bedenken gegen die externe Archivierung von Krankenunterlagen in codierten Containern geäußert. Insbesondere dürften diese Unterlagen nicht mehr dem Beschlagnahmeschutz gemäß § 97 Abs. 2 StPO unterfallen.

Meine Skepsis sehe ich durch ein Urteil des **OLG Düsseldorf** vom 20. August 1996 (20 V 139/95) bestätigt. In einem wettbewerbsrechtlichen Verfahren gegen ein Unternehmen, das die externe Archivierung und Mikroverfilmung für Krankenhäuser anbot, stellte das Gericht u.a. fest, daß das Aushändigen von Patientendaten an Dritte zur Archivierung eine Offenbarung im Sinne des § 203 Abs. 1 StGB darstelle. Zu deren Zulässigkeit sei eine Offenbarungsbefugnis erforderlich. Eine solche ergebe sich im Regelfall nur aus einer **ausdrücklichen Einwilligung** des Patienten. Außerdem sei die Beschlagnahmefreiheit gemäß § 97 Abs. 2 StPO bei einem externen Archivierungsunternehmen nicht gewährleistet.

3.4 Telemedizin

Auch die Entwicklung der Telemedizin schreitet fort. In meinem 17. Tätigkeitsbericht habe ich mich zu den rechtlichen Grundlagen und zum Aufbau des Bayerischen Gesundheitsnetzes im Rahmen der Initiative **Bayern Online** geäußert ([Nr. 3.1.2.](#)). Mittlerweile liegt der Abschlußbericht 1997 des Themenarbeitskreises "Telemedizin" - Bayerisches Gesundheitsnetz vor.

In diesem Themenarbeitskreis wird die Förderung von Projekten erörtert, bei denen personenbezogene Patientendaten über offene Netze versandt werden. Ich habe allen Beteiligten meine Vorstellungen über die in solchen Fällen erforderlichen Sicherheitsmaßnahmen zur Kenntnis gebracht. Von den Projektverantwortlichen wurde mir auch zugesichert, derartige Sicherheitsmaßnahmen bei Aufnahme des Echtbetriebs zu implementieren. Das Projekt "**Health Care Professional Protokoll**" der Kassenärztlichen Vereinigung Bayerns soll dazu die Voraussetzungen bieten (zum Projekt Basilika siehe [Nr. 19.3.1](#) dieses Tätigkeitsberichts). Im Berichtszeitraum wurde das Konzept für die hierfür erforderlichen Sicherheitsmaßnahmen entwickelt.

Für die Übertragung sensibler Patientendaten in offenen Netzen, wozu letztlich auch das Bayer. Behördennetz zählt, sind geeignete Sicherheitsmaßnahmen vorzusehen, damit die Vertraulichkeit und Integrität der übertragenen Daten sowie die Revisionsfähigkeit der Netzbenutzung und die Zugriffssicherheit der angeschlossenen DV-Systeme gewährleistet werden können. Dabei handelt es sich im wesentlichen um folgende Maßnahmenbündel:

- Das DV-System darf nur solchen Benutzern Zugang zum Netz erlauben, die sich sowohl als Berechtigte identifizieren können, als auch vom DV-System als Berechtigte erkannt werden (**Authentisierung**). Die berechtigten Benutzer können auch unterschiedliche Rechte besitzen. Als Zugangskontrollmedium ist beispielsweise die Chipkarte denkbar. Die Rechner, die die Verbindung zum Netz herstellen, und vor allem die internen Netze sind außerdem durch geeignete Sicherheitsmaßnahmen (Firewall-Konzepte) gegen Eindringversuche von außen (Veränderung von Software, Manipulation von Daten, Ausspähen von Informationen) abzusichern.
- Die **Integrität** der auf dem Netz übertragenen Daten läßt sich durch geeignete Signaturverfahren verifizieren. Es gibt bereits heute eine Reihe von Produkten, die diese Funktionalität leisten. Auch dazu lassen sich wiederum Chipkarten verwenden.
- Die **Vertraulichkeit** aller auf dem Netz übertragenen Daten muß durch geeignete Verschlüsselungstechniken gewährleistet werden. Dabei ist insbesondere zu beachten, daß die zum Einsatz kommenden Verfahren gegen Entschlüsselungsversuche hinreichend sicher sind. **Asymmetrische Verschlüsselungsverfahren** bieten hohe Sicherheiten. Auf die Ausführungen zu den kryptografischen Verfahren ([Nr. 19.3.1](#) dieses Tätigkeitsberichts) weise ich hin.
- Jedes angeschlossene DV-System muß für einen bestimmten Einzelfall zur **Beweissicherung** Empfangs- und Übergabenachweise aufzeichnen, damit erkennbar bleibt, wer wann an wen welche Daten übertragen hat (Protokollierung).

Ich habe das für telemedizinische Projekte zuständige Bayerische Staatsministerium für Arbeit

und Sozialordnung, Familie, Frauen und Gesundheit auf die besondere Bedeutung datenschutzgerechter Lösungen für die Akzeptanz telemedizinischer Anwendungen hingewiesen.

4. Sozialbehörden

4.1 Datenaustausch zwischen Sozialleistungsträgern untereinander bzw. mit Nicht-SGB-Stellen und Maßnahmen des Gesetzgebers zur Erweiterung solcher Befugnisse und Verpflichtungen

Die Kommunen beklagen, daß sie angesichts der immer schneller wachsenden Anzahl an Sozialhilfeempfängern zunehmend an die Grenzen ihrer finanziellen Leistungskraft stoßen. Mehr und mehr sehen sich sowohl die Verwaltung als auch die Politik angesichts knapper Finanzen veranlaßt, möglichst umgehend und möglichst effektiv schlagkräftige Erfolge bei der Bekämpfung des Sozialhilfe-/Sozialleistungsmissbrauchs vorweisen zu können.

Von Maßnahmen der Mißbrauchsbekämpfung werden aber nicht nur die "schwarzen Schafe", sondern auch der weitaus überwiegende Teil redlicher Sozialleistungsempfänger betroffen. Deshalb muß bei dieser Mißbrauchsbekämpfung darauf geachtet werden, daß die Verhältnismäßigkeit der Mittel gewahrt wird, d.h. daß einschneidende Maßnahmen zur Überprüfung und Mißbrauchsbekämpfung nur in Sozialleistungsbereichen eingesetzt werden, bei denen Mißbrauch in erheblichem Ausmaß feststellbar ist.

Von Datenschutz-Seite wird einer Verbesserung der Möglichkeiten zur Datenerhebung und -übermittlung nichts entgegengehalten, soweit diese Verbesserungen zur Einschränkung von Leistungsmissbräuchen erforderlich und verhältnismäßig sind. Es liegt nicht im Interesse eines recht verstandenen Datenschutzes, als Mantel für Leistungsmissbräuche zu dienen. Neue gesetzliche Kontrollbefugnisse - insbesondere zu verdachtsunabhängigen Datenabgleichen - sind aber dort nicht erforderlich, wo Sozialleistungsmissbrauch bereits unter **Anwendung vorhandener Ermittlungsmöglichkeiten** effektiv bekämpft werden kann. Bei der Frage, welche Datenerhebungen und -übermittlungen hierzu erforderlich sind, ist je nach Art und Umfang der Leistung und

nach dem Ausmaß des Leistungsmißbrauchs zu differenzieren: So wird möglicherweise die Mißbrauchsquote bei der Sozialhilfeverwaltung anders einzustufen sein als die Mißbrauchsquote im Bereich der Krankenkassen oder der Rentenversicherungsträger usw.

Für erforderlich halte ich **angemessene Datenerhebungen bei der Antragstellung - bzw. bei Dauerleistungen auch in angemessenen Zeitabständen danach -**, die eine Sozialbehörde vornimmt, um Angaben des Betroffenen zur Erlangung öffentlicher Leistungen zu überprüfen. Es scheint mir selbstverständlich, daß sich die Verwaltung nicht allein auf die Angaben des Betroffenen zu verlassen braucht, sondern solche Angaben auch nachprüfen darf. In diesem Zusammenhang ist vor allem der für den Sozialleistungsbereich generell geltende Untersuchungsgrundsatz nach § 20 SGB X, d.h. die Verpflichtung zur Aufklärung des Sachverhalts von Amts wegen, zu nennen. Für die Frage von Mißbrauchskontrollen kann im übrigen an nachvollziehbare grundsätzliche Lebens- oder Verwaltungserfahrungen hinsichtlich bestimmter Sachverhalte angeknüpft werden, die die jeweilige Verwaltung veranlassen (dürfen), in den einschlägigen Fällen Ermittlungen und Überprüfungen anzustellen. Je nach den Mißbrauchserkenntnissen im jeweiligen Sozialleistungsbereich braucht diese Beurteilung insoweit nicht zwingend auf die Umstände des zu bearbeitenden Einzelfalles beschränkt werden, sondern darf sich darüber hinaus auch an der den Sozialleistungsträgern unstreitig zukommenden Aufgabe orientieren, die "Funktionsfähigkeit des Ganzen" zu erhalten und dementsprechend die Erkennbarkeit unrechtmäßiger Leistungen bei der jeweiligen Fallbearbeitung durch angemessenen Datenaustausch sicherzustellen. Bei dieser Betrachtungsweise bedarf es jedenfalls insoweit keiner neuen Befugnis zu anlaßunabhängigen Datenerhebungen und -übermittlungen.

Anlaßunabhängige Datenerhebungen und -übermittlungen (wie z.B. in § 117 BSHG, vgl. Nr. 4.5.1) darf der Gesetzgeber nur für Sozialleistungsbereiche vorsehen, bei denen das erkennbare Ausmaß des Leistungsmißbrauchs einen solchen Datenaustausch erfordert und somit rechtfertigt, weil bereits vorhandene Kontrollinstrumentarien sich als zur effektiven Bekämpfung unzureichend erwiesen haben. Als Ausgleich für solche anlaßunabhängigen Kontroll- und Überwachungsmaßnahmen sind vom Gesetzgeber aber ggf. verfahrensmäßige Schranken für das Abgleichsverfahren festzusetzen, insbesondere Regelungen des Datenumfangs, der Zweckbindung und der Datenlöschung (wie in § 117 BSHG geschehen).

4.2 Vorschläge der Arbeitsgruppe der ASMK zu einem verbesserten Datenaustausch bei Sozialleistungen - Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20.10.1997

Die Konferenz der Ministerinnen und Minister, Senatorinnen und Senatoren für Arbeit und Soziales der Länder (ASMK) setzte 1995 eine länderoffene Arbeitsgruppe unter dem Vorsitz Bayerns ein und erteilte ihr den Auftrag zu prüfen, ob und in welchem Umfang im Bereich der Sozialleistungen Verbesserungen des Datenaustausches gefordert werden sollen (Behebung etwaiger Vollzugsdefizite bzw. Feststellung gesetzgeberischen Handlungsbedarfs).

Ich erhielt Gelegenheit, mich zum Bericht dieser Arbeitsgruppe zu äußern. Ich habe zu diversen Vorschlägen dieses umfangreichen Berichts Kritik erhoben, deren Darstellung im einzelnen den angemessenen Rahmen eines Beitrags im Tätigkeitsbericht überschreiten würde. Ich beschränke meine Berichterstattung deshalb darauf, daß ich federführend mit den Datenschutzbeauftragten des Bundes und der Länder die als [Anlage 9](#) dieses Tätigkeitsberichts abgedruckte Entschließung vom 20.10.1997 zu den Vorschlägen dieser ASMK-Arbeitsgruppe abgestimmt habe. Diese Entschließung geht auf einige Vorschläge des Berichts ein, gegen die aus datenschutzrechtlicher Sicht gravierende Bedenken anzumelden waren. Vor allem aber enthält die Entschließung Kritik daran, daß einzelne Vorschläge der ASMK-Arbeitsgruppe Veränderungen der Strukturen in der Verarbeitung personenbezogener Daten im Sozialleistungsbereich - insbesondere durch veränderte Verfahren der Datenerhebung - bewirken würden, ohne daß hinreichend geprüft und dargelegt wäre, ob minder schwere Eingriffe in das Persönlichkeitsrecht nicht ebenso zum Erfolg führen können. Etwaige neue Datenabgleichsverfahren müssen hinsichtlich ihrer Wirkungen bewertet werden; parallel zu ihrer Einführung ist daher die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies soll ermöglichen, Aufwand und Nutzen neuer Datenabgleichsverfahren zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen. Bei tatsächlich erforderlichen neuen Kontrollinstrumenten gegen den Leistungsmissbrauch muß dem davon potentiell betroffenen Bürger die Transparenz der Datenflüsse aufgezeigt werden, damit er nicht zum bloßen Objekt eines solchen Datenaustausches wird.

Auf ihrer 74. Konferenz im Herbst 1997 stellte die ASMK zum Bericht der Arbeitsgruppe fest, daß nach ihrer Auffassung im Bereich der Sozialleistungen Handlungsbedarf sowohl im Hinblick auf einen Mißbrauch ausschließenden Einsatz der begrenzten finanziellen Mittel als auch auf einen möglichst effektiven Vollzug besteht. Dieser Beschluß der 74. ASMK bezieht in erfreulicher Weise auch datenschutzrechtliche Belange ein, indem er auf die Abwägungsnotwendigkeit mit datenschutzrechtlichen Belangen hinweist und der Bundesregierung sowohl den Bericht der Arbeitsgruppe als auch die Entschließung der Datenschutzbeauftragten zur Prüfung übermittelt. Der Beschluß lautet auszugsweise wörtlich:

"... Die Ministerinnen und Minister, Senatorinnen und Senatoren für Arbeit und Soziales der Länder sind sich bewußt, daß im Einzelfall schwierige Güterabwägungen zwischen den Interessen der Solidargemeinschaften als Ganzem an einem zielgenauen Ressourceneinsatz und den Interessen der einzelnen Leistungsempfänger bzw. Antragsteller an der Wahrung ihres informationellen Selbstbestimmungsrechts zu treffen sind und daß beide Güter gleichberechtigt nebeneinander stehen. ... Die Ministerinnen und Minister ... bitten die Bundesregierung, die erforderlichen Schritte zur Realisierung eines verbesserten Datenaustauschs in diesem Sinne in die Wege zu leiten, dabei unter Einschluß des Gesprächsangebotes der Datenschutzbeauftragten den Bericht der Arbeitsgruppe und die Entschließung der Datenschutzbeauftragten des Bundes und der Länder ... in die Prüfung einzubeziehen und der ASMK bis zum nächsten Jahr zu berichten. Die Länder sagen zu, alle geeigneten Maßnahmen für eine Verbesserung des Datenaustauschs unter Beachtung des Rechts der informationellen Selbstbestimmung zu ergreifen und fordern auch die Vollzugsbehörden auf, entsprechend tätig zu werden."

4.3 Gesetzesantrag des Freistaats Bayern: "Entwurf eines Gesetzes zur Schaffung von Arbeitsanreizen und zur Vermeidung von Mißbrauch in der Sozialhilfe" (BR-Drs. 388/98 vom 29.04.1998)

Als Reaktion auf den vorstehend zitierten Beschluß der 74. ASMK brachte Bayern beim Bundesrat den Entwurf eines Gesetzes zur Schaffung von Arbeitsanreizen und zur Vermeidung von Mißbrauch in der Sozialhilfe ein. Dieser Gesetzesentwurf wurde vom Bundesrat bis Redaktions-

schluß dieses Tätigkeitsberichts nicht an den Deutschen Bundestag herangetragen. Ich erhielt im Vorfeld des Gesetzesantrags Gelegenheit zur Stellungnahme und habe u.a. folgende Kernpunkte angesprochen:

Änderung des § 16 Abs. 1 BSHG: Vermutung der Bedarfsdeckung

Der geltende § 16 BSHG stellt eine eingeschränkte und widerlegbare gesetzliche Vermutung auf, daß in einer Haushaltsgemeinschaft zusammenlebende **verwandte oder verschwägte** Personen gegenseitig den Bedarf für den Lebensunterhalt decken. Die vorgeschlagene Neufassung des § 16 BSHG sieht die **Erweiterung dieser Vermutung auf alle Personen vor, die gemeinsam Wohnraum bewohnen**. Zwar sollen laut Begründung zum Gesetzesentwurf "Wohngemeinschaften herkömmlicher Art" (bei denen lediglich Nebenräume wie Bad und Küche mitbenutzt werden) nicht unter die Neufassung des § 16 BSHG fallen; andererseits aber soll eine ganze oder teilweise Bedarfsdeckung des Betroffenen durch Mitbewohner vermutet werden, wenn diese anderen Personen finanziell dazu in der Lage sind und der äußere Umstand des gemeinsamen Bewohnens von Wohnraum vorliegt. Die vorgeschlagene Vermutung der Bedarfsdeckung geht m.E. datenschutzrechtlich deshalb zu weit, weil damit alle Personen, bei denen diese Vermutung einschlägig ist, zu Auskünften nach § 116 Abs. 1 BSHG über ihre Einkommens- und Vermögensverhältnisse verpflichtet wären; nach dem Entwurf eines § 116 Abs. 2 a BSHG - auf den ich anschließend noch eingehen werde - müßten **Kreditinstitute** dem Sozialhilfeträger über alle solchen Mitbewohner sogar für einen Zeitraum von bis zu 10 Jahren vor der Sozialhilfe-Antragstellung des Betroffenen zurück Auskünfte erteilen.

Nach dem bisher vorgeschlagenen Wortlaut des § 16 BSHG wäre womöglich bereits dann eine Vermutung der Bedarfsdeckung gegeben, wenn ein Sozialhilfeempfänger mit einem begüterten Studenten in einer Wohngemeinschaft lebt und berechtigt ist, dessen Wohnzimmer (beispielsweise zum gelegentlichen Fernsehen) mitzubedenutzen. Sowohl der begüterte Student als auch unter gleichen Wohn- bzw. Lebensverhältnissen etwa der Vermieter bei einem Untermietverhältnis wären verpflichtet, nach Maßgabe des § 116 Abs. 1 Satz 3 BSHG dem Sozialhilfeträger über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben und das Sozialamt könnte nach Maßgabe des § 116 Abs. 2 a BSHG (vorgeschlagene Neufassung) etwa Bankauskünfte bis zu 10 Jahren vor der Antragstellung zurück einholen. Sobald diese datenschutzrechtli-

chen Konsequenzen im Falle der Gesetzesänderung allgemein bekannt werden, dürfte die Bereitschaft wohl deutlich abnehmen, einen Sozialhilfeempfänger in eine Wohngemeinschaft oder zur Untermiete aufzunehmen.

Zwar läßt sich die Vermutung der gegenseitigen Bedarfsdeckung widerlegen. Es ist aber für das Sozialamt problematisch, von außen zu beurteilen, ob die Anwesenheit eines Hilfesuchenden in den Räumen des Dritten (gemeinsames Bewohnen) nur **gelegentlich** erfolgt; zum anderen müssen in der Praxis wohl gewisse "Hürden" für die Widerlegung der Vermutung aufgestellt werden, weil die Vermutung andernfalls ihren Zweck nicht erfüllen würde, dem Sozialamt die Sachverhaltserforschung maßgeblich zu erleichtern. Selbst wenn laut Gesetzesbegründung "kein zu strenger Maßstab" an die Widerlegung der Vermutung angelegt werden soll, dürfte es den Betroffenen vielfach doch schwerfallen, Anscheinsbeweise dafür zu liefern, daß eine Bedarfsdeckung **nicht** erfolgt. Da die erweiterte Vermutung eine effektive Arbeitserleichterung für die Sozialämter darstellen soll, dürfte die Auffassung des Sozialministeriums in der Praxis kaum realisierbar sein, wonach zur Widerlegung der Vermutung häufig schon eine glaubhafte Versicherung des Hilfesuchenden und des Dritten, daß Leistungen des Dritten an den Hilfesuchenden nicht erbracht werden, zur Abwendung der Auskunftspflicht genügen würde.

Zum Entwurf des § 116 Abs. 2 a BSHG: Auskunftspflicht Dritter über Guthaben und Vermögensgegenstände

Nach dieser Bestimmung würde dem Sozialhilfeträger ein Auskunftsanspruch über 10 Jahre zurück insbesondere gegen **Kreditinstitute** eingeräumt werden, die für einen Hilfesuchenden/-empfänger, die Unterhaltspflichtigen und ihre nicht getrennt lebenden Ehegatten sowie für die im gleichen Haushalt lebenden Personen Guthaben führen oder Vermögensgegenstände verwahren. Daß diese neue Auskunftspflicht gegenüber Personen, die mit dem Hilfeempfänger in den gleichen Wohnräumen leben (Entwurf zur Erweiterung des § 16 BSHG) zu weitgehend wäre, habe ich bereits dargelegt.

Für das in der Gesetzesbegründung genannte Ziel dieser 10 Jahre zurückgreifenden Auskunftspflicht, nämlich damit das Sozialamt Rückforderungsansprüche eines inzwischen verarmten Schenkers nach § 528 BGB realisieren kann, erscheint mir dieser Anspruch außerdem wenig

tauglich. Hinsichtlich einzelner Bankauskünfte über weiter zurückliegende Zeitpunkte werden sich die Betroffenen - ohne daß dies vom Sozialamt widerlegt werden könnte - vielfach auf mangelnde Erinnerung berufen, so daß der Sozialhilfeträger mit der Auskunft über eine bestimmte Guthabenshöhe zu einem bestimmten Zeitpunkt wenig wird anfangen können; außerdem wird die Nachweisführung über die Richtigkeit oder Unrichtigkeit seiner Angaben auch für einen redlichen Hilfeempfänger mit zunehmendem Zeitraum seit der Zuwendung immer schwieriger. Die Person, die eine Vermögenszuwendung erhalten hat, ist selbst nicht auskunftspflichtig.

Nun scheint mir das Sozialministerium allerdings davon auszugehen, daß die Banken durch § 116 Abs. 2 a BSHG verpflichtet würden, **alle Kontoauszüge** bis zu 10 Jahren vor der Antragstellung zurück vorzulegen. Diese Auffassung des Sozialministeriums würde sich m.E. nicht mit dem Bankgeheimnis vereinbaren lassen, man bedenke, welche Menge an Informationen das Sozialamt dabei über Dritte (z.B. Überweisungsempfänger) erfahren würde. Auch § 315 Abs. 2 und 5 SGB III, denen der vorgeschlagene § 116 Abs. 2 a BSHG nachgebildet wurde, verpflichtet die Banken m.E. nicht zu Auskünften über alle Kontenbewegungen sowie Herkunft, Zielrichtung und Verwendungszwecke der Geldflüsse. Beschränkt man aber - wie dies in den Auskunftersuchen der Bundesanstalt für Arbeit an Kredit- und Versicherungsinstitute (§ 315 SGB III) der Fall ist - die Auskunft auf eine bestimmte Guthabenshöhe zu einem bestimmten Zeitpunkt, sind meine Einwendungen gegen die vorgeschlagene 10-Jahres-Frist bei Auskünften an Sozialhilfeträger durchaus einschlägig.

**Ergänzungen der §§ 67 a Abs. 1 und 69 Abs. 1 SGB X: Datenerhebungen und -
übermittlungen zur Mißbrauchskontrolle setzen einen Anfangsverdacht nicht voraus**

Zu diesem (auf die Vorschläge der ASMK-Arbeitsgruppe zurückgehenden) Gesetzesantrag wird zunächst nochmals auf die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20.10.1997 verwiesen (vgl. vorangehende Nr. und Anlage 9 dieses Tätigkeitsberichts). Anders als die Gesetzesvorlage zu vermitteln versucht, handelt es sich im Falle dieser Gesetzesergänzung keineswegs lediglich um "Klarstellungen" im SGB X, sondern um tiefgreifende Veränderungen im Recht des Sozialdatenschutzes: Die Erforderlichkeit im Einzelfall als Voraussetzung für die Erhebung und Übermittlung von Sozialdaten würde faktisch aufgegeben und der Sozialdatenschutz bliebe hinter dem Schutz sonstiger Bürgerdaten nach dem Bundesdaten-

schutzgesetz und den Datenschutzgesetzen der Länder zurück. Mit der pauschalen Begründung "Mißbrauchskontrolle" dürften **alle vom Geltungsbereich des SGB X erfaßten Sozialleistungsträger**, d.h. auch alle Sozialversicherungsträger, Sozialdaten erheben, ohne daß noch kontrollierbar wäre, ob die Datenerhebung erforderlich und i.S.d. Übermaßverbots angemessen war. Konkrete Erkenntnisse dafür, daß es **bei allen SGB-Stellen** Leistungsmißbrauch in einem Umfang gibt, der anders als durch diese Gesetzesergänzung nicht mehr effektiv bekämpft werden könnte, also Anzeichen für einen alle Sozialleistungsträger betreffenden massenweisen Mißbrauch, sind mir nicht bekannt. Hierzu verweise ich auch auf meine Ausführungen unter [Nr. 4.1.](#)

4.4 Allgemeines zum Begriff "(Sozial-)Datenabgleich"

Immer häufiger ist von Datenabgleichen bzw. von Sozialdatenabgleichen die Rede, sei es, daß die Forderung erhoben wird, solche Abgleiche für bestimmte Sachverhalte gesetzlich im einzelnen zu regeln oder daß lediglich gefordert wird, bereits vorhandene Befugnisse zum Datenabgleich auszuschöpfen.

Ich könnte mir vorstellen, daß weiten Kreisen gar nicht geläufig ist, was unter dem Begriff "Datenabgleich" eigentlich zu verstehen ist. Dies möchte ich hier in Grundzügen erläutern und außerdem ganz allgemein einige rechtliche Zusammenhänge beim Datenabgleich aufzeigen:

Unter einem Datenabgleich verstehe ich die Überprüfung eines oder mehrerer Sachverhalte (Datum/Daten) anhand mindestens eines identischen Indexes, meistens anhand der Identität einer zu überprüfenden Person; ein solcher Datenabgleich ist etwa innerhalb eines Arbeitsbereichs oder zwischen Arbeitsbereichen einer oder mehrerer Behörden denkbar. Beispiele sind, daß die Rentensachbearbeitung eines Rentenversicherungsträgers bei der Arbeitseinheit "Rehabilitation" desselben Trägers abgleicht, ob ihre im Zuge der Aufgabenerfüllung erforderlichen Erkenntnisse (Sozialdaten) über einen Versicherten mit den Daten übereinstimmen, über die die Arbeitseinheit "Rehabilitation" verfügt. Oder: Ein Sozialamt fragt bei der Krankenkasse eines Antragstellers oder Sozialhilfebeziehers nach, ob die Krankenkasse bestätigt, daß eine Krankengeldzahlung den Angaben des Betroffenen entsprechend tatsächlich abgelehnt oder eingestellt wurde.

Datenschutzrechtlich relevant ist dabei u.a., daß ein personenbezogener Datenabgleich seitens der Arbeitseinheit, die den Abgleich initiiert, in aller Regel Elemente einer Datenbeschaffung/Datenerhebung und zugleich einer Datenoffenbarung/Datenübermittlung enthält, letzteres nämlich zumindest über die Tatsache, daß zwischen dieser Stelle und dem Betroffenen ein dienstlicher Kontakt besteht. Die befragte Arbeitseinheit soll daraufhin im Rahmen des Datenabgleichs die ihr bekannten Umstände der anfragenden Einheit mitteilen, sei es, daß sie selbst den Abgleich durchgeführt hat (Ergebnismitteilung), sei es, damit die anfragende Stelle ihrerseits den Abgleich durchführen kann.

Soweit der Datenabgleich zwischen selbständigen speichernden Stellen i.S.d. [Art. 4 Abs. 9 BayDSG](#), § 67 Abs. 9 SGB X erfolgt und deshalb Datenerhebungen und Datenübermittlungen zum Inhalt hat, müssen deren Zulässigkeitsvoraussetzungen nach [Art. 16 BayDSG](#) (Datenerhebung) bzw. nach [Art. 18 BayDSG](#) (Datenübermittlungen) gegeben sein. Soweit für die Datenerhebung und -verarbeitung einer oder beider beteiligten Stellen spezialgesetzliche Regelungen wie etwa Vorschriften des SGB einschlägig sind, gehen diese den Regelungen des BayDSG vor. Wenn der Datenabgleich ausschließlich zwischen Arbeitseinheiten stattfindet, die keine selbständigen speichernden Stellen sind (z.B. weil sie keine SGB-Stellen i.S.d. § 67 Abs. 9 Satz 3 SGB X sind) und deshalb **die Behörde** als speichernde Stelle gilt, liegen (lediglich) Datennutzungen vor, die nach [Art. 17 BayDSG](#) oder nach vorrangigen Spezialvorschriften über die Datennutzung zulässig sein müssen.

Grundsätzlich ist zum Datenabgleich noch zu erwähnen, daß er zur **Aufgabenerfüllung** mindestens der initiiierenden Stelle **erforderlich** sein muß; diese Erforderlichkeit ist sowohl hinsichtlich des Umfangs der Informationsbeschaffung und -verwendung von Bedeutung als auch in aller Regel für die Frage, ob ein Datenabgleich überhaupt zulässig ist. Sofern keine spezialgesetzlichen Regelungen wie etwa § 117 BSHG auch **anlaßunabhängige** Datenabgleiche erlauben, sind Datenabgleiche nur bei konkretem Anlaß als erforderlich anzusehen. Ein solcher Anlaß kann u.a. darin liegen, daß Angaben des Betroffenen, die er in seinem Antrag auf Leistungen öffentlicher Stellen macht, auf ihre Richtigkeit und Vollständigkeit überprüft werden müssen, etwa weil die vom Betroffenen selbst vorgelegten Unterlagen zur Nachweisführung nicht ausreichen oder z.B. weil konkrete Anhaltspunkte für unrichtige bzw. unvollständige Angaben die Be-

hörde zu Ermittlungen veranlassen, die nicht oder jedenfalls nicht allein mit dem Betroffenen bewerkstelligt werden können.

4.5 Sozialhilfeverwaltung

4.5.1 Sozialhilfedatenabgleichsverordnung zu § 117 Abs. 1 und 2 BSHG

Nach § 117 Abs. 1 und 2 Bundessozialhilfegesetz (BSHG) sind die Sozialhilfeträger befugt, Beziehender von Sozialhilfeleistungen auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen, ob und in welcher Höhe und für welche Zeiträume von ihnen Leistungen der Bundesanstalt für Arbeit oder der Träger der gesetzlichen Unfall- oder Rentenversicherung (**Auskunftsstellen**) oder auch BSHG-Leistungen durch andere Träger der Sozialhilfe bezogen werden oder wurden und in welchem Umfang Zeiten des BSHG-Leistungsbezuges mit Zeiten einer Versicherungspflicht oder Zeiten einer geringfügigen Beschäftigung zusammentreffen. Auf diese Weise sollen Fälle von Sozialhilmifemißbrauch aufgedeckt werden, in denen der Betroffene gegenüber dem Sozialamt unrichtige oder unvollständige Angaben über anderweitigen Leistungsbezug oder über eine (auch geringfügige) Beschäftigung gemacht hat. Zur Realisierung des automatisierten Datenabgleichs nach § 117 Abs. 1 und 2 BSHG bedurfte es einer Rechtsverordnung; diese "Sozialhilfedatenabgleichsverordnung - SozhiDAV -" ist nunmehr (endlich) zum 01.01.1998 in Kraft getreten und ermöglicht viermal jährlich Datenabgleiche - erstmals im April 1998 - für das jeweils vorangegangene Kalendervierteljahr (Abgleichszeitraum). Diese Datenabgleiche sind "auch regelmäßig", d.h. ohne konkrete Anhaltspunkte auf Leistungsmißbrauch, zulässig. Der Gesetzgeber verspricht sich von diesen Datenabgleichsbefugnissen u.a. einen allgemeinen Abschreckungseffekt gegenüber potentiell Mißbrauchswilligen.

Die Datenübermittlung durch die Sozialhilfeträger an die Auskunftsstellen erfolgt über die Datenstelle der Rentenversicherungsträger (DSRV, einer Abteilung des Verbandes Deutscher Rentenversicherungsträger) als **Vermittlungsstelle**. Übermittelt werden dürfen dabei gemäß § 117 Abs. 1 Satz 2 BSHG im wesentlichen lediglich identifizierende Daten und Zuordnungsdaten zum Sozialhilfeträger.

Aus datenschutzrechtlicher Sicht galt es insbesondere sicherzustellen, daß die Datenstelle der Rentenversicherungsträger nach Abschluß ihrer Aufgaben beim Datenabgleich **zur unverzüglichen Löschung der zum Abgleichsverfahren dort temporär gespeicherten Daten verpflichtet** wurde. Durch die jetzige Fassung des § 117 Abs. 2 a BSHG und des § 15 Abs. 2 Sätze 2 und 3 SozhiDAV ist geregelt, daß die Vermittlungsstelle keine dauerhaft oder auch nur unnötig lang bestehende Zentraldatei über Sozialleistungen führt. Nach der aktuellen Fassung der Sozialhilfedatenabgleichsverordnung tritt darüber hinaus für Auskunftsstellen an die Stelle der ursprünglich vorgesehenen Löschungsfristen die unverzügliche Löschung der Datensätze nach Erhalt einer empfangsquittierenden Rückmeldung der Vermittlungsstelle.

Desweiteren erhält bzw. erstellt die Vermittlungsstelle, wenn kein Leistungsbezug, keine Zeiten einer Versicherungspflicht und keine Zeiten einer geringfügigen Beschäftigung festgestellt wurden, keinen personenbezogenen Antwortdatensatz für das Sozialamt; der Antwortdatensatz enthält in diesen Fällen lediglich ein "Erkennungszeichen", das der Vermittlungsstelle eine Zuordnung zum zuständigen Sozialhilfeträger ermöglicht und das nur dieser dem betreffenden Sozialhilfeempfänger zuordnen kann. Auch so wird dem Anliegen Rechnung getragen, daß die Daten der Sozialhilfeempfänger nur solange, wie es für den Abgleich unbedingt erforderlich ist, bei der DSRV aufbewahrt werden.

Aus datenschutzrechtlicher Sicht lege ich großen Wert darauf, **daß zu belastenden Feststellungen aus dem Sozialhilfedatenabgleich zuerst dem Leistungsempfänger Gelegenheit zur Stellungnahme gegeben wird**, bevor der Sozialhilfeträger Erkundigungen bei dritten Personen oder Stellen einholen darf. Diese Auffassung der Datenschutzbeauftragten wurde vom Bundesministerium für Gesundheit bestätigt und in die Begründung zu § 14 SozhiDAV aufgenommen. Werden dem Sozialhilfeträger nämlich Überschneidungen zurückgemeldet, bedeutet dies nicht zwangsläufig, daß Sozialhilfemißbrauch vorliegt. Dies gilt insbesondere bei Feststellungen, die auf einem Abgleich mit der Datei der geringfügigen Beschäftigungsverhältnisse bei der DSRV beruhen (§ 11 Abs. 4 SozhiDAV). Als "Feststellungen" müssen dem Sozialhilfeträger zwar alle Fälle gemeldet werden, bei denen im Abgleichszeitraum Zeiten geringfügiger Beschäftigungen gespeichert sind, es ist aber anerkannt, daß die Datei der geringfügig Beschäftigten objektiv fehlerträchtig ist (vgl. Steinmeyer in: Wannagat, § 150 SGB VI, Rdnr. 12); belastende Feststellun-

gen aus der Datei der geringfügig Beschäftigten sind daher stets unter Vorbehalt zu nutzen. Diese Datei enthält möglicherweise in einer nicht unbedeutenden Anzahl von Fällen wegen mangelnder Abmeldung durch den Arbeitgeber nicht mehr zutreffende Angaben.

Das zu § 117 BSHG gefundene Verfahren zeigt, daß Mißbrauchskontrolle und datenschutzgerechte Ausgestaltung ihrer Umsetzung durchaus keinen Widerspruch darstellen müssen.

4.5.2 Sozialhilfedatenabgleich nach § 117 Abs. 3 BSHG, u.a. mit der Kfz-Zulassungsstelle

Zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe ermöglicht § 117 Abs. 3 BSHG den Sozialhilfeträgern - wiederum verdachtsunabhängig -, Daten von Leistungsbeziehern u.a. bei ihren wirtschaftlichen Unternehmen und bei diversen anderen Stellen der Verwaltung zu überprüfen. Dabei ist die Überprüfung folgender "Katalogdaten" zulässig: Geburtsdatum und -ort; Personen- und Familienstand; Wohnsitz; Dauer und Kosten von Miet- oder Überlassungsverhältnissen von Wohnraum; Dauer und Kosten von bezogenen Leistungen über Elektrizität, Gas, Wasser, Fernwärme oder Abfallentsorgung; Eigenschaft als Kraftfahrzeughalter.

Hierzu weise ich insbesondere auf folgendes hin:

Die soeben genannten Katalogdaten dürfen meines Erachtens nur bei den Stellen abgeglichen werden, bei denen diese Daten sozusagen in originärer Zuständigkeit gespeichert sind, wie etwa hinsichtlich der Angaben Geburtsdatum und -ort, Personen- und Familienstand sowie Wohnsitz beim **Einwohnermeldeamt** bzw. hinsichtlich der Eigenschaft als Kraftfahrzeughalter bei der **Kfz-Zulassungsstelle**. Für unzulässig erachte ich dagegen eine Anfrage nach Name, Anschrift und Geburtsdatum eines Betroffenen z.B. bei der Unterhaltsvorschußkasse, wenn diese Anfrage letztlich nicht zur Überprüfung der Aktualität oder Übereinstimmung dieser Daten erfolgt, sondern dem Sozialamt primär die Erkenntnis verschaffen soll, ob über den betroffenen Sozialleistungsbezieher ein Vorgang bei der Unterhaltsvorschußkasse existiert ("Etiketten-Schwindel"). Da § 117 Abs. 3 BSHG als Spezialnorm generell verdachtsunabhängige Überprüfungen erlaubt, müssen die Datenabgleiche streng auf die Katalogdaten beschränkt werden; darüber hinausgehende Überprüfungen - wie etwa nach Leistungen der Wohngeldstelle - sind nicht nach dieser

Norm, sondern nach Maßgabe des § 67 a SGB X anlaßabhängig zulässig, vgl. zu letzterer Frage [Nr. 4.3](#)

Bei der Kfz-Zulassungsstelle ist nach § 117 Abs. 3 BSHG lediglich die Überprüfung der "Eigenschaft als Kraftfahrzeughalter" erlaubt. Darüber hinausgehende Auskünfte an das Sozialamt, z.B. über Automarke, Typ und Alter des Kfz gestatten weder das BSHG noch das StVG. Stellt das Sozialamt bei dieser Überprüfung die Eigenschaft eines Leistungsbeziehers als Kraftfahrzeughalter fest, müssen die näheren Einzelheiten im Rahmen der Mitwirkungspflichten mit dem Hilfeempfänger geklärt werden. Diese Auffassung hat auch das Sozialministerium mit Schreiben vom 08.11.1994 (Az.: IV 2/7101/4/94) an die kreisfreien Städte und Landkreise vertreten.

Ich räume ein, daß die derzeitige Fassung dieser BSHG-Befugnis zur Kfz-Halter-Abfrage den Anforderungen der täglichen Praxis in der Sozialhilfeverwaltung möglicherweise nicht ausreichend gerecht wird; so dürfte die Mitwirkungspflicht des Betroffenen nach § 60 SGB I z.B. kaum mehr realisierbar sein, wenn der Sozialhilfebezug bereits beendet ist und lediglich überprüft werden soll, ob Leistungen in der Vergangenheit unrechtmäßig bezogen und zurückgefordert werden können bzw. müssen. Die geltende Rechtslage läßt aber nur zu, daß dem Sozialamt ausschließlich mitgeteilt wird, ob ein Leistungsbezieher Kraftfahrzeughalter ist oder nicht ("Ja/Nein").

Eine Änderung dieser Rechtslage hielte ich aus datenschutzrechtlicher Sicht für bedenkenfrei.

4.5.3 Datenaustausch Sozialamt-Polizei

Anfang 1997 führten Presseberichte über eine Dienstanweisung für das Sozialamt der Landeshauptstadt München zu einer ebenso heftigen wie kontroversen öffentlichen Diskussion. Es ging um die Fragen, ob Mitarbeiter des Sozialamts auch damals schon verpflichtet waren, der Polizei im Wege der Amtshilfe zu melden, daß sich gesuchte Straftäter zum Zeitpunkt des Auskunftsernehmens gerade in den Diensträumen des Sozialamts aufhalten oder welcher Vorsprachetermin dem Sozialamt bereits bekannt ist und ob die Polizei informiert werden müsse, sobald der Betroffene wieder im Sozialamt erscheint.

Die Auskunft, daß der Betroffene bei einer Sozialbehörde vorspricht, enthält auch die Information, daß zwischen dem Betroffenen und dem Amt ein Kontakt besteht, der die Aufgabenerfüllung der Sozialbehörde zum Gegenstand hat. Somit enthalten solche Informationen Sozialdaten und dürfen an Dritte, auch an die Polizei, nur dann weitergegeben werden, wenn das Sozialgesetzbuch (SGB) es erlaubt.

Unstreitig war bei dieser Diskussion von Anfang an, daß der Polizei die gegenwärtige oder künftige Vorsprache einer gesuchten Person in der Sozialbehörde mitgeteilt werden darf,

- nach § 69 Abs. 1 SGB X, wenn die zur Last gelegte Straftat im Zusammenhang mit der Gewährung von Sozialleistungen steht, beispielsweise bei Sozialhilfe-Betrug und
- nach § 73 SGB X, wenn es "zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist" und ein Richter diese Auskunft angeordnet hat.

Auch durfte der Polizei bereits seinerzeit gemäß § 68 Abs. 1 SGB X u.a. "der derzeitige Wohnsitz" mitgeteilt werden. Ich habe - was in der Kommentarliteratur und von den Datenschutzbeauftragten überwiegend abgelehnt wurde - u.a. mit Rücksicht auf ein Urteil des Kammergerichts Berlin vom 26.05.1983 ("gegenwärtiger Aufenthalt als Minus zur derzeitigen Anschrift") nicht beanstandet, daß darunter auch noch der "gegenwärtige Aufenthalt in der Sozialbehörde" fällt.

Darüber hinaus teilte das Staatsministerium für Arbeit und Sozialordnung den Sozialbehörden in seinem Rundschreiben vom 05.02.1997 aber mit, daß Sozialamtsbedienstete die Polizei nach § 68 SGB X auf Nachfrage auch über künftige Vorsprachen der Betroffenen im Amt zu benachrichtigen hätten; ferner sei die Polizei auf eine frühere Anfrage hin zu benachrichtigen, sobald der Betroffene im Amt vorspricht oder einen Termin vereinbart. In seiner Pressemitteilung vom 06.02.1997 teilte das Sozialministerium hierzu mit, daß die Regierungen mit dem Rundschreiben "angewiesen" werden, "die Amtshilfe der Sozialämter für die Polizeibehörden bei der Fahndung nach Straftätern sicherzustellen".

Gemäß [Art. 31 Abs. 1 BayDSG](#) habe ich diese Anordnung insoweit beanstandet und vom Sozialministerium die datenschutzgerechte Korrektur seiner Anweisung gefordert, weil sich die im

vorstehenden Absatz genannten Auskünfte an die Polizei nicht auf § 68 SGB X (damaliger Fassung) stützen ließen. Informationen über - gemessen am Auskunftersuchen - künftige Behördenkontakte sind **keine Auskünfte über die "derzeitige Anschrift des Betroffenen" mehr**, sondern weitergehende, von § 68 SGB X nicht mehr erfaßte Datenübermittlungen.

Da die Landeshauptstadt München der Aufforderung der Regierung von Oberbayern nicht nachkam, gemäß der - von mir beanstandeten - Weisung des Sozialministeriums zu handeln, wurde die Stadt durch die Regierung von Oberbayern insoweit ihrerseits rechtsaufsichtlich beanstandet.

Weil das Sozialministerium und die Regierung von Oberbayern meinen datenschutzrechtlichen Forderungen nicht nachkamen, habe ich mich in dieser Situation gem. [Art. 31 Abs. 2 Satz 3 BayDSG](#) erstmals an den Landtag und an die Staatsregierung gewandt. Die Staatsregierung und der Landtag haben sich meiner Rechtsauffassung nicht angeschlossen.

Mittlerweile wurde § 68 SGB X erweitert und läßt nunmehr auch die von mir beanstandeten Fallgestaltungen von Auskünften für Zwecke der Amtshilfe zu. Die Sozialausschüsse im Bundestag und Bundesrat erhielten im parlamentarischen Gesetzgebungsverfahren keine Gelegenheit, sich mit dieser erweiterten Auskunftspflicht und ihren Folgen für die praktische Arbeit der Sozialleistungsträger auseinanderzusetzen, weil die Erweiterung des § 68 SGB X erst im Rahmen der Beratungen des dort federführenden Gesundheitsausschusses zu einem "Ersten Gesetz zur Änderung des Medizinproduktegesetzes" in dieses Gesetz, hinter dem niemand eine Änderung des Sozialgesetzbuchs vermuten würde, eingebracht wurde.

Diese Gesetzeserweiterung, wonach der Polizei im Einzelfall auf Ersuchen auch der zukünftige Aufenthalt (etwa in der Behörde) bekanntzugeben ist und wonach entsprechende Auskunftersuchen beim Sozialleistungsträger bis zu 6 Monate gespeichert werden dürfen, wurde leider nicht auf Sozialbehörden beschränkt, die Sozialleistungen ausschließlich aus Steuermitteln bezahlen, sondern erfaßt auch die Sozialversicherung wie z.B. die gesetzlichen Krankenkassen, die Renten- und Unfallversicherungsträger usw. Auch die Jugendämter können zur Mitfahndung herangezogen werden, obwohl gerade diese Ämter zu ihrer Aufgabenerfüllung besonders auf das Vertrauen ihrer Klientel angewiesen sind. Da die Gesetzeserweiterung auch nicht etwa auf Personen

beschränkt wurde, die mit Haftbefehl gesucht werden, kann sich die Polizei künftig zur Erfüllung aller ihrer Aufgaben der Sozialbehörden bedienen, etwa bei der Suche nach Zeugen und bei der Erstellung von Bewegungsbildern im Rahmen der polizeilichen Beobachtung.

Ich werde die künftige Handhabung polizeilicher Auskunftersuchen an Sozialleistungsträger und die Probleme, die den Sozialbehörden bei der Beantwortung in praktischer und rechtlicher Hinsicht entstehen, aufmerksam beobachten:

Nach wie vor ist die Übermittlungsbefugnis nach § 68 SGB X auf Ersuchen im Einzelfall beschränkt, so daß jedenfalls Regelanfragen oder ganze Fahndungslisten bei den Sozialleistungsträgern unzulässig sind. Wie bisher hat der ersuchte Sozialleistungsträger die Grenzen der Amtshilfe nach § 4 Abs. 3 SGB X zu beachten, insbesondere wenn durch die Hilfeleistung die Erfüllung seiner eigenen Aufgaben ersichtlich gefährdet würde. Über § 4 Abs. 3 SGB X hinaus ist die ersuchte Sozialbehörde nach § 68 Abs. 1 Satz 2 SGB X zur Auskunftserteilung auch dann nicht verpflichtet, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann; zu dieser Überprüfung durch den Sozialleistungsträger bedarf es entsprechender Aussagen bereits im Auskunftersuchen. Wie bisher darf ferner kein Grund zur Annahme bestehen, daß durch die Auskunftserteilung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Dieser Abwägungsklausel könnte nunmehr beispielsweise in Fällen, in denen die Suchmitteilung nicht Beschuldigte, sondern etwa Zeugen betrifft, oder bei Ordnungswidrigkeitenverfahren erhöhte Bedeutung zukommen.

Die Beobachtungen der Praxis sollen auch zeigen, ob sich die allgemeine Aussage in der Kommentarliteratur, bei der Verfolgung von Straftaten gäbe es kein überwiegendes Interesse des Einzelnen an der Nichtoffenbarung der in § 68 SGB X genannten Angaben, auf die nunmehr erweiterten Mitteilungsmöglichkeiten ohne weiteres übertragen läßt oder ob angemessene Differenzierungen angezeigt sind.

4.5.4 Einsatz von Sozialhilfeermittlern

In zunehmendem Ausmaß setzen die Träger der Sozialhilfe vor allem zur Bekämpfung mißbräuchlicher Inanspruchnahme von Sozialhilfeleistungen Außendienstmitarbeiter ein, die teilweise sogar speziell zu diesem Zweck eingestellt wurden, so etwa Polizeibeamte im Ruhestand, die in Teilzeittätigkeit für das Sozialamt ermitteln.

Ich gehe nach den Bestimmungen des SGB X von folgenden datenschutzrechtlichen Grundsätzen für den Einsatz dieser Mitarbeiter aus:

1. Der Einsatz eines Außendienstes zur Prüfung, ob die gesetzlichen Voraussetzungen des Leistungsbezugs gegeben sind, ist möglich, soweit diese Art der Datenerhebung erforderlich und verhältnismäßig ist.

Gemäß § 37 Satz 3 SGB I geht das Zweite Kapitel des SGB X (Sozialdatenschutz) dessen Erstem Kapitel (Verwaltungsverfahren) vor, soweit sich die Ermittlung des Sachverhalts nach den §§ 20 und 21 SGB X auf Sozialdaten erstreckt. Die Grenzen der Datenerhebung bestimmen sich deshalb nach § 67 a SGB X (siehe dazu die nachfolgenden Nummern 3, 4 und 5).

2. Die Verhältnismäßigkeit dieses Einsatzes ist sowohl im Vergleich zu weniger beeinträchtigenden Ermittlungsmöglichkeiten als auch ggf. hinsichtlich des Gewichts bereits vorliegender Verdachtsmomente auf Sozialhilfe-Mißbrauch zu überprüfen.

Unter dem Gesichtspunkt der Verhältnismäßigkeit kommen als weniger eingreifend vorrangig andere Ermittlungsmöglichkeiten wie z.B. die schriftliche Befragung des Betroffenen, dessen Einbestellung ins Amt oder die in § 117 BSHG vorgesehenen Datenabgleiche in Betracht.

Sozialhilfe-Ermittler sollten jedenfalls nur mit genau definiertem Auftrag der Sachbearbeiter/-innen und regelmäßig nur gegenüber Betroffenen (vgl. nachfolgende Nr. 4) einge-

setzt werden. Voraussetzung für die Maßnahmen sind konkrete Erhebungsanlässe, insbesondere **konkrete Anhaltspunkte für Sozialhilfe-Mißbrauch**; für einen Ermittlereinsatz zur Verdachtsfindung fehlt es am Kriterium der Erforderlichkeit gegenüber dem Betroffenen.

3. Bei der Befragung haben die Ermittler dem Betroffenen die erforderlichen Informationen zu geben über Name und Dienststelle des Ermittlers, den Zweck seines Besuches sowie die Angaben, inwieweit der Betroffene zu Auskünften verpflichtet ist (ggf. nach welcher Vorschrift) oder seine Angaben freiwillig sind; im Falle der Auskunftspflicht ist er auf die Folgen der Verweigerung hinzuweisen (vgl. § 67 a Abs. 3 SGB X).

Sozialhilfe-Ermittler dürfen keinen Zutritt zur Wohnung des Betroffenen erzwingen oder mit falschen Angaben (Vorwänden) erreichen. Der Ermittler muß im Hinblick auf Art. 13 GG (Unverletzlichkeit der Wohnung) klarstellen, daß der Betroffene nicht verpflichtet ist, ihm den Zutritt zur Wohnung zu gestatten. Leistungsversagung oder Leistungsentzug nach § 66 SGB I dürfen bei Zutrittsverweigerung allenfalls dann angedroht bzw. realisiert werden, wenn die erforderliche Sachverhaltsermittlung ohne Zutritt zur Wohnung nicht durchführbar ist. Dies bedarf sorgfältiger Überprüfung.

4. Bei dritten Personen oder Stellen dürfen die Sozialhilfe-Ermittler Daten über den Betroffenen nur nach Maßgabe der in § 67 a Abs. 2 Satz 2 Nr. 2 SGB X genannten Voraussetzungen erheben, insbesondere also, wenn die Aufgabe ihrer Art nach eine Erhebung bei Dritten (z.B. bei einem Zeugen) erfordert. Dabei haben die Ermittler insbesondere die Verhältnismäßigkeit dieser Form der Datenerhebung, die ohne Mitwirkung des Betroffenen erfolgt, zu prüfen.

Im Falle des § 67 a Abs. 2 Satz 2 Nr. 2 b SGB X dürfen auch keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Dieser gesetzlichen Regelung liegt die Überlegung zugrunde, daß Datenerhebungen bei Dritten in Sozialleistungsangelegenheiten für den Betroffenen erhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung bedeuten. Viele Menschen

empfinden vor allem den **Kontakt zu Sozialhilfebehörden** als abwertend. Gerade bei der Befragung Dritter durch Mitarbeiter des Sozialamts läßt sich aber vielfach nicht vermeiden, daß die Befragten durch Tatsache, Art und Inhalt der Erhebungen über solche Kontakte - und darüber hinaus über Verdachtsmomente unkorrekten Verhaltens des Betroffenen - Kenntnis erlangen. Die Abwägung, ob deshalb Anhaltspunkte für die Beeinträchtigung **überwiegender** schutzwürdiger Interessen des Betroffenen bestehen oder ob das **öffentliche Interesse** an der Datenerhebung bei Dritten **überwiegt**, kann nicht pauschal, sondern nur anhand der Umstände des Einzelfalls erfolgen. Datenerhebung bei Dritten darf dabei aber nicht zum Regelfall werden.

Eine Datenerhebung aus allgemein zugänglichen Quellen - wie z.B. durch Ablesen von Klingel-Schildern an der Haustüre, durch Adreßbuch- oder Telefonbuch-Recherchen - stellt keine Datenerhebung bei "anderen Personen oder Stellen" dar und ist deshalb zulässig.

Soweit Sozialhilfe-Ermittler den Betroffenen bei Hausbesuchen nicht antreffen, und daraufhin andere Mitbewohner oder Nachbarn **ausschließlich** fragen, wann der Betroffene voraussichtlich wieder anzutreffen sei, brauchen sie gegenüber diesen Personen weder ihre Dienststelle noch den Zweck ihres Besuchs offenbaren. Bereits bei der Einholung solcher Auskünfte Hinweise nach § 67 a Abs. 3 SGB X (vgl. oben Nr. 3, 1. Abs.) zu verlangen, würde mehr "Schaden" hervorrufen als "korrektes Verfahren" bewirken.

5. Gegen eine verdeckte Beobachtung ("Beschattung") durch Sozialhilfe-Ermittler bestehen größte Bedenken. Dies gilt lediglich nicht für **Ausnahmefälle** kurzfristiger Beobachtung - etwa ob der Betroffene zur Arbeit geht -, **wenn ein konkreter, auf Tatsachen begründeter Verdacht besteht und alle anderen Erkenntnismittel nicht zum Ziel führen.**

Eine derartige, auf engste Ausnahmefälle beschränkte kurzfristige Beobachtung unter Berücksichtigung des konkreten Tatverdachts und der Schwere des zur Last gelegten Delikts sollte auf alle Fälle schriftlich und durch den Leiter des Sozialamts selbst angeordnet werden, ebenso ihr zeitlicher Umfang und die enge Begrenzung des Erhebungsgegen-

stands.

Als Schwerpunktaufgabe und Regelmaßnahme von Sozialhilfe-Ermittlern muß die verdeckte Personenbeobachtung ausscheiden. Die "Beschattung" als massiver Eingriff in das Recht auf informationelle Selbstbestimmung führt regelmäßig auch zu zusätzlichen Erkenntnissen aus der Privatsphäre der Betroffenen, die nicht Gegenstand der Ermittlungen sind. Die Betroffenen sind der Beschattung entsprechend deren Zielsetzung wehrlos ausgeliefert. Eine der Schwere des Eingriffs entsprechende normenklare Befugnis zur Beschattung enthält das SGB X nicht. Eine verdeckte Beobachtung auf der Grundlage der allgemeinen Datenerhebungsbefugnis nach § 67 a SGB X ist regelmäßig unzulässig. Den Einsatz von **"Sozialhilfe-Detektiven" mit dem Aufgabenschwerpunkt Personen-Observierung halte ich daher für unzulässig.**

6. In allen Fällen des Einsatzes von Sozialhilfe-Ermittlern ist eine Notiz über Anlaß und Zweck des Einsatzes, über die Legitimation gegenüber Betroffenen und über ihnen erteilte Belehrungen sowie über Verlauf und Ergebnis des Einsatzes notwendig, die zum Sozialhilfe-Akt genommen werden soll. Bei formularmäßiger Vorbereitung solcher Notizen dürfte sich der Aufwand für die Aktenvermerke in Grenzen halten. Diese Dokumentationen erachte ich für wesentlich, da sie die Datenschutzkontrolle solcher Erhebungen und die Aufsichtsführung durch die Sozialhilfeverwaltung ermöglichen. Außerdem bedarf es dieser Notizen zur Erteilung von Auskunftsansprüchen der Betroffenen nach § 83 SGB X.

Die soeben dargelegten Gesichtspunkte habe ich auch dem Bayerischen Landkreistag, dem Bayerischen Städtetag und dem Verband der Bayerischen Bezirke zugeleitet mit der Bitte, aus der Sicht der kommunalen Praxis dazu Stellung zu nehmen. Der Bayerische Städtetag hat sich grundsätzlich gegen den Einsatz von sog. "Sozialhilfe-Ermittlern mit quasi detektivischen Aufgaben" ausgesprochen. In diesem Sinne hat sich auch der Verband der Bayerischen Bezirke geäußert. Beide Gremien vertreten hierzu u.a. die Auffassung, daß dem Sozialhilfemißbrauch durch Prävention im Sinne einer intensivierten Sachbearbeitung mit noch besser ausgebildetem Personal vorgebeugt werden sollte, und verweisen auch auf die Befugnisse zum Datenabgleich nach

§ 117 Bundessozialhilfegesetz i.V.m. der Sozialhilfedatenabgleichsverordnung (vgl. [Nr. 4.5.1](#) und [4.5.2](#)). Ich begrüße diese Sicht.

4.5.5 Sozialdatenschutz und Sachleistungsgewährung nach dem Bundessozialhilfegesetz

Die Gewährung von Sachleistungen ist nach dem Bundessozialhilfegesetz (BSHG) ausdrücklich erlaubt und im Grundsatz auch nach dem Recht des Sozialdatenschutzes zulässig.

Knapper werdende Sozialhilfemittel berechtigen die Sozialhilfeträger, im Rahmen der Verhältnismäßigkeit Verwaltungsverfahren zu praktizieren, die eine gerechte Verteilung der Mittel sicherstellen und Leistungsreduzierungen für alle Hilfeempfänger vermeiden helfen. So können ökonomische Gründe und wirtschaftlicher Druck für den Abschluß von **Rahmenverträgen** mit Lieferanten und Dienstleistern (z.B. Möbel- und Elektrofirmen, Speditionen usw.) unter Vereinbarung von besonders preisgünstigen Konditionen und - als Gegenleistung - **Abnahmekontingenten** sprechen, die durch Sachleistungsgewährung zu realisieren sind. Selbstverständlich haben aber auch Sozialhilfeempfänger Anspruch auf die Beachtung ihres informationellen Selbstbestimmungsrechts, d.h. die Abwicklung der Sachleistungsgewährung muß den Anforderungen des Sozialdatenschutzes entsprechen.

1. Vor seiner Entscheidung über die Verfahrensmodalitäten der Sachleistungsgewährung hat der Sozialhilfeträger in seine Gesamtabwägung datenschutzgerecht einerseits die Interessen des **betroffenen Hilfeempfängers** einzubringen, andererseits aber auch die Interessen der **Gesamtheit der Hilfeempfänger** sowie der Allgemeinheit insbesondere an einer sparsamen Verwendung öffentlicher Mittel und die sich daraus für ihn ergebenden Pflichten. Dies gilt auch für die Erfahrung vieler Sozialhilfeträger, wonach ein nicht unerhebliches Risiko besteht, daß mit BSHG-Sachleistungen ein reger Handel, also Sozialhilfemißbrauch betrieben wird.

Bei seinen Überlegungen zur Ausgestaltung des Sachleistungsverfahrens muß der Sozialhilfeträger auch berücksichtigen, daß ihm das BSHG hinsichtlich der Form der Sozialhil-

fe einen Ermessensspielraum und das Sozialdatenschutzrecht hinsichtlich der Beurteilung der Erforderlichkeit von Datenübermittlungen einen gewissen Abwägungsspielraum einräumen und daß eine Maßnahme deshalb nicht rechtswidrig ist, soweit er die Grenzen dieser Spielräume nicht überschreitet.

Der Sozialdatenschutz soll und darf nicht dazu führen, daß **angemessene** Leistungskontrollen zum Schaden der Allgemeinheit verhindert werden und mißbrauchsbekämpfende Maßnahmen ohne zwingende Notwendigkeit unterbleiben müssen.

2. Aus datenschutzrechtlicher Sicht folgt daraus, daß die Entscheidung des Sozialhilfeträgers, ob eine nach dem BSHG zulässige Sachleistungsgewährung **die Weitergabe personenbezogener Daten des Hilfeempfängers an die Vertragsfirma erfordert oder nicht**, insbesondere nach den vorstehenden Kriterien sachgerecht differenziert und abgewogen sein muß:

Erfordert die Lieferung und/oder Montage bzw. der Anschluß der jeweiligen Bedarfsgegenstände die Weitergabe von Name und Adresse des Hilfeempfängers wie etwa bei größeren, schwereren Gegenständen wie Elektrogeräten, Waschmaschinen, Herden usw., ist diese Datenübermittlung an die Vertragsfirma zulässig, vgl. hierzu allerdings Nr. 3.

Ob und inwieweit die Erbringung der Sachleistungen in anderen Fällen dagegen mittels **Wertgutscheinen** erfolgen kann, die zwar (z.B. durch ein Aktenzeichen) für die Abrechnung individualisierbar, für die Vertragsfirma aber **nicht identifizierend** sind, oder inwieweit auch hier eine Sozialdatenübermittlung erforderlich ist, damit die Firma die Identität des Empfängers zur Mißbrauchsbekämpfung prüfen kann, muß der Sozialhilfeträger jeweils nach den sachlichen und örtlichen Verhältnissen seines Zuständigkeitsbereiches entscheiden.

Grundsätzlich erscheint mir dabei die Verwendung **identifizierender** Wertgutscheine vertretbar, wenn der jeweilige Sozialhilfeträger in seinem Zuständigkeitsbereich ohne Identitätsprüfung **schon bei der Ausgabe** der Sachleistungen Leistungsmißbrauch in ei-

nem erheblichen Umfang annehmen muß und soweit er es deshalb nicht verantworten kann, Sachleistungen ohne Identitätsprüfung auszugeben und sich so dem Vorwurf u.a. seitens der Rechnungsprüfung auszusetzen, seinen Kontrollverpflichtungen nicht ausreichend nachzukommen.

Soweit Sozialhilfeträger aber bei Sachleistungsgewährung Sozialdaten an Vertragsfirmen weiterzugeben beabsichtigen, verlange ich **zum Ausgleich solcher Eingriffe** in das informationelle Selbstbestimmungsrecht und aus Gründen der Transparenz, daß die Betroffenen rechtzeitig **Hinweise** im Sinne der nachstehenden Nr. 3 erhalten:

3. Da Sozialhilfeleistungen in aller Regel umgehend benötigt werden, wird und muß der Sozialhilfeträger die bewilligte Sachleistung bei der Lieferfirma ebenso umgehend - und nach den o.g. Kriterien erforderlichenfalls unter Offenbarung der Identität des Hilfeempfängers - bestellen, damit der Artikel sofort ausgeliefert werden kann, sobald der Betroffene bei der Vertragsfirma vorspricht.

Wenn der Hilfeempfänger dem Sozialhilfeträger aber belegt, daß er die beantragten Leistungen **gleich günstig oder sogar günstiger selbst beschaffen kann, ist nach dem BSHG-Leistungsrecht eine Barleistung zu erbringen**, soweit nicht im Einzelfall eine zweckwidrige Verwendung des Geldbetrags zu befürchten ist.

Der **Betroffene** muß daher **frühzeitig** angeben, daß er vorrangig eine Barleistung wünscht **und** bereit ist, dem Sozialhilfeträger Unterlagen für einen Kostenvergleich vorzulegen, damit der Leistungsträger davon absieht, die Lieferfirma umgehend unter Übermittlung von Sozialdaten über den Sachleistungsbezug zu informieren.

Dies wiederum setzt voraus, daß der **Sozialhilfeträger** ggf. frühzeitig und in geeigneter Form darauf **hinweist**,

- daß und welche Sozialdaten er bei der Sachleistungsgewährung alsbald an die Vertragsfirma weiterzugeben beabsichtigt,

- unter welchen Voraussetzungen er von der Sachleistungserbringung zugunsten einer Barleistung absieht und dementsprechend auch keine identifizierenden Daten an den Vertragspartner übermittelt sowie
- daß sich der Betroffene umgehend äußern muß, wenn er die Sachleistungserbringung und die Datenweitergabe (insbesondere durch das Ermöglichen eines Kostenvergleichs) vermeiden will, ggf. unter Inkaufnahme der dadurch entstehenden Verzögerung der Leistungsgewährung.

4.6 Jugendämter

4.6.1 Sicherstellung des Datenschutzes bei Trägern der freien Jugendhilfe

Im Berichtszeitraum habe ich mich auch mit der Frage befaßt, wie § 61 Abs. 4 SGB VIII in die Praxis umgesetzt werden kann. Diese Vorschrift lautet: "Werden Einrichtungen und Dienste der Träger der freien Jugendhilfe in Anspruch genommen, **so ist sicherzustellen**, daß der Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung und Nutzung in entsprechender Weise gewährleistet ist."

Wie ich erfahren habe, bereitet die Umsetzung und Auslegung dieser Vorschrift in der Praxis der Jugendhilfe Schwierigkeiten. Zur Umsetzung des § 61 Abs. 4 SGB VIII schlage ich deshalb insbesondere die folgenden "sicherstellenden Maßnahmen" i.S. dieser Vorschrift vor:

1. Zwischen dem Träger der öffentlichen und dem Träger der freien Jugendhilfe ist (über die Regelung der fachlichen Aufgabenübertragung hinaus) ein **gesondertes Kooperationspapier zur Sicherstellung und Gewährleistung des Sozialdatenschutzes** zu vereinbaren. Diese formale Trennung soll den eigenständigen Charakter der datenschutzrechtlichen Verpflichtungen betonen.

2. In diesem Datenschutz-Kooperationspapier ist beispielsweise zu konkretisieren, welche Vorgänge dem Jugendamt bei welchen Fallgestaltungen im Zuge der Verfahrensabwicklung vorzulegen sind.

Für näher zu bestimmende "heikle Fälle", insbesondere wenn die Übermittlung personenbezogener Daten an andere Stellen eine **Zweckänderung** gegenüber der Datenerhebung beinhaltet, sollte eine Rückfrage beim Jugendamt nach der Zulässigkeit der beabsichtigten Datenübermittlung vorgesehen werden.

3. Zur Sicherstellung der Verantwortung für die Gewährleistung des Sozialdatenschutzes nach § 61 Abs. 4 SGB VIII hat sich das Jugendamt gegenüber dem freien Jugendhilfe-Träger im Datenschutz-Kooperationspapier

- weitere Detailregelungen sowie
- Zustimmungserfordernisse (z.B. für die Einrichtung und Ausgestaltung einer Statistik)

- soweit erforderlich - vorzubehalten.

4. Darüberhinaus sollte im Kooperationspapier festgelegt werden, daß die Mitarbeiter des Trägers der freien Jugendhilfe durch geeignete, möglichst langjährige Mitarbeiter des Jugendamts in der Anwendung der Vorschriften über den Sozialdatenschutz zu unterrichten sind; dabei sollten den betreffenden Mitarbeitern des freien Jugendhilfe-Trägers insbesondere **praktische Problemfälle** aus den Erfahrungen des Jugendamts vermittelt werden.
5. Weitere Inhalte des Kooperationspapiers könnten Vorgaben zur internen Nutzungsbeschränkung (§ 35 Abs. 1 Satz 2 SGB I) sowie zur Datenlöschung (bzw. -berichtigung und -sperrung) nach § 84 SGB X sein.

6. Der freie Jugendhilfe-Träger sollte zu konkreten Datensicherungsmaßnahmen i.S.d. § 78 a SGB X verpflichtet werden.

Ich bin mir bewußt, daß diese Vorschläge lediglich eine Art Gliederung eines solchen Kooperationspapiers darstellen und daß es einen erheblichen Arbeitsaufwand bedeutet, die Inhalte der Gliederungspunkte im einzelnen auszuarbeiten. Hierzu dürfte auch die Klärung diverser fachlicher Jugendhilfefragen notwendig sein. Wünschenswert wäre die Erstellung eines Musters eines solchen gesonderten Kooperationspapiers zur Sicherstellung und Gewährleistung des Sozialdatenschutzes durch eine Arbeitsgruppe, die mit Experten aller fachlich tangierten Bereiche und länderübergreifend besetzt ist.

Darüberhinaus kommt es in Betracht, Träger der freien Jugendhilfe künftig auch in Pflegesatzvereinbarungen bzw. in Kosten- oder Finanzierungsbescheiden zur entsprechenden Gewährleistung des Sozialdatenschutzes zu verpflichten; bei den genannten Bescheiden könnte dies in Form eines Widerrufsvorbehalts bzw. einer Auflage als Nebenbestimmung zum Verwaltungsakt erfolgen.

4.7 Gesetzliche Krankenversicherung

4.7.1 Datenträgeraustausch zwischen Krankenkassen und Kassenzahnärztlichen Vereinigungen

Unter [Nr. 4.2.3](#) meines 17. Tätigkeitsberichts - 1996 - habe ich mich zum seinerzeitigen Sachstand und zur datenschutzrechtlichen Problematik bei Datenübermittlungen von der Kassenzahnärztlichen Vereinigung Bayerns (KZVB) an die gesetzlichen Krankenkassen zu Abrechnungszwecken geäußert. Hierzu kann ich mittlerweile über die Realisierung erheblicher datenschutzrechtlicher Verbesserungen berichten.

Gemäß § 295 Abs. 2 i.V.m. § 285 Abs. 4 Sozialgesetzbuch - SGB - V dürfen die KZVen den Krankenkassen für jedes Quartal die für die vertragszahnärztliche Versorgung erforderlichen

Angaben über die abgerechneten Leistungen lediglich fallbezogen, nicht aber versichertenbezogen übermitteln. Dadurch soll der Aufbau vollständiger personenbezogener Krankheitskonten verhindert werden. Da eine Vereinbarung nach § 295 Abs. 3 SGB V über "das Nähere über Einzelheiten des Datenträgeraustausches" zwischen den Spitzenverbänden der Krankenkassen und der Kassenzahnärztlichen Bundesvereinigung nicht zustandekam, setzte das Bundesschiedsamt für die vertragszahnärztliche Versorgung mit Schiedsspruch vom 20.02.1995 den Umfang der Datenübermittlung für Abrechnungszwecke zwischen KZVen und gesetzlichen Krankenkassen als "Vertrag über den Datenaustausch auf Datenträgern" fest.

Die in dem Schiedsspruch zu Abrechnungszwecken vorgesehenen Datenübermittlungen ließen sich jedoch mit § 295 Abs. 2 SGB V nicht vereinbaren; die uneingeschränkte Umsetzung des Schiedsspruchs hätte nämlich dazu geführt, daß die Versicherten aus den von den KZVen zu übermittelnden Abrechnungsdaten durch die Krankenkassen ohne Schwierigkeit hätten reidentifiziert werden können, wenn man den pro Behandlungsfall zu erstellenden Einzelfallnachweis (Datensatz mit dem Nachweis der von jedem Vertragszahnarzt abgerechneten Leistungen, § 1 Abs. 3 des Vertrags) mit dem ebenfalls pro Behandlungsfall zur Prüfung der Leistungspflicht der Krankenkasse nach § 284 Abs. 1 Nr. 4 SGB V zu erstellenden (versichertenbezogenen) Datensatz (§ 2 des Vertrags) EDV-technisch verknüpft hätte. Diese Verknüpfung ließ sich aufgrund einiger in beiden Datensätzen identisch enthaltener Angaben realisieren.

In Gesprächen des Bundesbeauftragten für den Datenschutz mit der Kassenzahnärztlichen Bundesvereinigung und mit den Spitzenverbänden der gesetzlichen Krankenkassen - die von einer internen Diskussion der Datenschutzbeauftragten vorbereitet bzw. begleitet wurden - konnten wesentliche datenschutzrechtliche Korrekturen dieses Datenträgeraustauschvertrags erzielt werden. So enthalten die Datensätze nach § 2 des Vertrags (s.o.) keine Angaben über den "Fallwert in Punkten und DM" mehr, die sich auch aus dem Einzelfallnachweis (§ 1 Abs. 3 des Vertrags) errechnen ließen und die eine Verknüpfung der beiden Datensätze maßgeblich erleichterten. Den entscheidenden Durchbruch bei den Verhandlungen des Bundesbeauftragten für den Datenschutz sehe ich jedoch darin, daß sie zur Vereinbarung einer sog. "Protokollnotiz" zum o.g. Datenträgeraustauschvertrag führten. In dieser "Protokollnotiz" wurde unter Punkt 4 vereinbart, daß bei der Leistungsabrechnung der Kassenzahnärztlichen Vereinigungen mit den Krankenkassen der

Zahnarzt grundsätzlich nicht identifiziert werden muß: Die von den KZVen an die Kassen zu übermittelnden Einzelfallnachweise enthalten danach Zahnarztnummern ausschließlich in **codierter** Form; die Datensätze zur Prüfung der Leistungspflicht (§ 2 des Vertrags) enthalten - anders als im Schiedsspruch vorgesehen - keinerlei Zahnarztnummern. Dadurch ist nunmehr gewährleistet, daß eine Personalisierung der Patienten (aber auch der Zahnärzte) durch ein Verknüpfen der beiden Abrechnungsdatensätze nicht zu erreichen ist.

Nur in begründeten Fällen und unter Angabe des Verwendungszwecks ist der Krankenkasse auf ihr Verlangen ein einzelner abrechnender Zahnarzt zu benennen. Wenn die Krankenkasse von der KZV die Angabe des Zahnarztnamens verlangt hat, wird die Zahnarztnummer neu verschlüsselt.

Wie weitere Nachfragen bei der Kassenzahnärztlichen Vereinigung Bayerns ergaben, war das Risiko, daß die Codierung der Zahnarztnummer im Abrechnungsdatensatz durch eine Zusammenführung der Abrechnungsdatensätze **mit zahnarztbezogenen Datensätzen für die Auffälligkeitsprüfung** die ihr zugeschriebene Sicherungs- und Sperrwirkung verlieren könnte, jedenfalls bei einer großen KZV wie derjenigen in Bayern bereits äußerst gering. Um auch dieses Restrisiko auszuschließen, codiert die KZVB nunmehr die Zahnarztnummern je Quartal und je Kasse verschieden.

Im Ergebnis kann ich also mitteilen, daß aufgrund dieser erzielten Verhandlungsergebnisse jedenfalls in meinem Zuständigkeitsbereich nicht mehr zu befürchten steht, daß die zahnärztlichen Abrechnungsdaten aufgrund der Umsetzung des Datenträgeraustauschvertrags in einer Art und Weise an die Krankenkassen übermittelt werden, die dort gesetzlich nicht erlaubte Reidentifizierungen von Patienten durch Verknüpfung von Abrechnungsdaten ermöglicht.

Die im Bereich des Datenaustauschs zwischen Kassenzahnärztlicher Vereinigung und gesetzlicher Krankenversicherung gewonnenen Erkenntnisse machen m.E. im Bereich des automatisierten Datenaustauschs zwischen den Kassenärztlichen Vereinigungen und der GKV ebenfalls Nachbesserungen notwendig. Wie sich mittlerweile allerdings auch in anderen Ländern gezeigt hat, läßt sich dies de facto nur durch entsprechende Vereinbarungen zwischen der Kassenärztli-

chen Bundesvereinigung und den Spitzenverbänden der gesetzlichen Krankenversicherung, also auf Bundesebene, lösen. Die Verhandlungen, die der Bundesbeauftragte für den Datenschutz mit den genannten Vertragspartnern aufgenommen hat, dauern noch an.

4.7.2 Erweiterung der Krankenversichertenkarte (KVK) zur Bekämpfung des Mißbrauchs bei Medikamentenverschreibung

Seit Einführung der KVK brauchen die Versicherten nicht nur keinen Krankenschein, sondern auch keinen Überweisungsschein mehr. Von verschiedenen Seiten wird beklagt, daß dadurch sowohl medizinisch unbegründete Mehrfachbesuche bei (verschiedenen) Ärzten als auch unnötige und teilweise sogar vorsätzlich erschlichene Mehrfach-Verordnungen von Arzneimitteln (wie z.B. Codein-Hustensaft) drastisch zugenommen hätten.

Die Krankenkassen, die gemäß § 12 Abs. 1 Satz 2 SGB V keine Leistungen bewilligen dürfen, die nicht notwendig oder unwirtschaftlich sind, haben nach hiesiger Erkenntnis bisher keine Möglichkeit, ein solches Erschleichen von Medikamenten frühzeitig zu erkennen und dagegen vorzugehen; bisher erfahren die Krankenkassen von solchen Mißbräuchen erst, wenn ihnen die Rezepte seitens der Apotheken zur Abrechnung vorgelegt werden.

Aufgrund dessen wird zunehmend auch die Frage erörtert, ob eine künftige Generation der KVK zur Bekämpfung des Mißbrauchs bei Medikamentenverschreibungen eingesetzt werden kann, indem man sie als "intelligente Chipkarte" ausgestaltet und sie um Speicherungsmöglichkeiten für medizinische Daten ergänzt. Der technische Fortschritt und die Kostensenkung für Speicher- und Prozessorchip-Karten fördern solche Überlegungen zusätzlich.

Über die Aufnahme medizinischer Daten in die KVK muß der Gesetzgeber entscheiden, da der Karteninhalt in § 291 SGB V abschließend festgelegt ist.

Dabei wären folgende datenschutzrechtliche Fragen zu berücksichtigen:

Die bisherige Beschränkung des KVK-Inhalts auf Verwaltungsdaten bewirkt, daß der Kassenpatient bei der Inanspruchnahme ärztlicher Leistungen trotz gesetzlicher Verpflichtung zur Vorlage der KVK (§ 15 Abs. 2 SGB V) nicht gezwungen ist, dem Arzt mehr Informationen über sich zu geben, als er freiwillig möchte. So ist es ihm möglich, z.B. Angaben über erfolgte Arztbesuche oder Verordnungen zu verschweigen; in vielen Fällen, etwa wenn der Patient zu gravierenden ärztlichen Diagnosen, zur Erforderlichkeit von Operationen oder auch zur Verträglichkeit verordneter Medikamente eine ärztliche Zweitmeinung einholen möchte, muß ein solches Verhalten auch keineswegs mißbräuchlich sein. Wie sich daran zeigt, führt die Idee der Speicherung von Medikamentenverschreibungen auf der KVK mitten in die datenschutzrechtliche Diskussion, die zur Verwendung freiwilliger Chipkarten im Gesundheitswesen bereits geführt wird (vgl. im [16. TB Nr. 2.7](#) und im [17. TB Nr. 3.1.1](#)). Es ist kaum anzunehmen, daß dem Patienten aufgrund technischer Differenzierungen die Möglichkeit verbleibt, bei der Vorlage der KVK darauf gespeicherte Medikationshinweise zu unterdrücken, weil diese Unterdrückungsmöglichkeit dem Zweck zuwiderlaufen würde, gerade durch die Verpflichtung zur KVK-Vorlage Medikamentenmißbrauch zu unterbinden.

Außerdem werden aus den auf der KVK gespeicherten Daten über die Verordnung und Verabreichung von Medikamenten **erhebliche Rückschlüsse auf den Gesundheitszustand** des Karten-Inhabers möglich sein. Der Patient wäre vermutlich z.B. bei hautärztlicher Behandlung wegen Fußpilz gezwungen, dem Hautarzt ggf. die Einnahme von Psychopharmaka zu offenbaren; beim Abholen der verordneten Hautcreme in der Apotheke wäre diese Offenbarung erneut unumgänglich. Später würde dann außerdem der Nervenarzt vom Fußpilz des Patienten erfahren ...

Ob Medikamentenmißbrauch oder medizinisch unbegründete Mehrfachbesuche von Ärzten ein Ausmaß erreichen, das zur Angemessenheit und Verhältnismäßigkeit einer derartigen KVK-Erweiterung auf medizinische Daten durch den Gesetzgeber führt, wäre seitens der Krankenkassen und Kassen(zahn)ärztlichen Vereinigungen darzulegen. Andernfalls gehe ich davon aus, daß die große Mehrheit redlicher Kassenpatienten nicht zur Vorlage medizinischer Daten mittels der KVK gezwungen werden sollte. Ist der erste Schritt erst getan, steht im übrigen zu befürchten, daß über Verwaltungsdaten hinaus bald auch weitere medizinische Daten (als Pflichtdaten) auf der KVK gespeichert werden sollen.

Sollte sich der Gesetzgeber trotzdem für die Aufnahme der Medikationsdaten in die KVK und für die Verpflichtung zur Vorlage dieser Informationen entschließen, müßte der KVK angesichts der "Auslagerung medizinischer Patientendaten" auf die Versicherten (die die Karte ja mit sich herumtragen) ein dem Arztgeheimnis entsprechender Schutz von Patientendaten gesichert werden. Die 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat für den Bereich freiwilliger Patientenchipkarten bereits eine Entschlieung zur Sicherstellung des Schutzes medizinischer Datenbestände auerhalb von rztlichen Behandlungseinrichtungen gefat (vgl. Anlage 8 zu diesem TB); erst recht mte der Gesetzgeber die **Patientendaten auf der KVK** entsprechend dem **Arztgeheimnis** schtzen, wenn er Kassenpatienten gesetzlich dazu verpflichtet, ihre medizinischen Daten in Form der KVK selbst aus dem Schutzbereich des Arztgeheimnisses herauszutragen.

4.8 Medizinischer Dienst der Krankenversicherung (MDK)

4.8.1 EDV-Verfahren "ISmed-Neu"

Unter [Nr. 4.4.1](#) meines 17. Ttigkeitsberichts - 1996 - habe ich ber meine datenschutzrechtliche Prfung bei der Hauptverwaltung des MDK in Bayern berichtet. Zu den seinerzeit offenen Fragen kann ich ber folgende weitere Entwicklungen berichten:

a. Automatisierte Gutachtenspeicherung:

Der MDK darf nach den §§ 276 Abs. 2 Satz 6 SGB V/97 Abs. 3 Satz 3 SGB XI **in Dateien** nur Angaben zur Person und **Hinweise** auf bei ihm vorhandene Akten aufnehmen. In Dateien drfen - wie bereits berichtet - ber die bliche Abwicklungsdauer eines Begutachtungsverfahrens (mit EDV-untersttzter Gutachtenerstellung) hinaus automatisiert auswertbare medizinische Begutachtungsergebnisse nur so gespeichert werden, da **keine Identifizierung der begutachteten Personen mehr mglich ist.**

Mittlerweile sind meine diesbezglichen Bedenken bezglich der "Statistik-Datei" und der "Statistik-Datei Pflege" im DV-System "ISmed", das den MDK in den Lndern

vom Medizinischen Dienst der Spitzenverbände (MDS) einheitlich zur Verfügung gestellt wird, ausgeräumt; die genannten Statistik-Datensätze können mit Ausnahme eines geringen Rest-Risikos, das vernachlässigt werden darf, maschinell nicht mit Identitätsdaten betroffener Patienten verknüpft werden, d.h. bei der Hauptverwaltung des MDK und/oder im jeweiligen Beratungszentrum ist maschinell keine Reidentifizierung der in den Statistik-Dateien anonymisiert gespeicherten Angaben zum begutachteten Versicherten zu befürchten.

Auf mein Betreiben werden die Statistiksätze in den jeweiligen Beratungszentren nach Versand ihrer Kopien an die Hauptverwaltung mittlerweile nicht mehr 6 Monate lang aufbewahrt, sondern bereits nach 5 Werktagen ab Diskettenversand über einen sog. "Löschlauf" automatisch gelöscht.

Anschließend sind die Statistiksätze aller Beratungszentren bei der Hauptverwaltung nur noch gesammelt und unselektiert 2 bis 4 Monate lang in einer großen Datenbank vorhanden.

b. Mitteilung des Untersuchungsergebnisses an die gesetzliche Krankenkasse:

Nach § 277 Abs. 1 SGB V hat der MDK der Krankenkasse das **Ergebnis** der Begutachtung und "die erforderlichen Angaben über den Befund" mitzuteilen. Mein Anliegen war, daß der MDK an die Krankenkasse eine inhaltlich auf das gesetzlich vorgesehene Maß reduzierte Version des MDK-Gutachtens weiterleitet, während das ausgedruckt zur Archivierung beim MDK vorgesehene Gutachten-Exemplar im Hinblick auf evtl. Folgebegutachtungen detaillierter gehalten werden kann. Bisher war eine technische Variierung des Gutachtenumfangs ohne manuellen Löschungsaufwand und damit im Ergebnis schon aufgrund des Zeit- und Arbeitsaufwands beim MDK nicht möglich. Meine gemeinsamen Bemühungen mit dem Bundesbeauftragten für den Datenschutz (BfD) führten mittlerweile zu einem ersten Erfolg: Das EDV-Verfahren, das der MDS den MDKs der Länder zur Verfügung stellt, wurde u.a. dahingehend überarbeitet, daß MDK-Gutachten nunmehr je nach Verwendungszweck inhaltlich variiert werden können. Diese technische Verbesserung stellt m.E. einen bedeutenden Fortschritt zur datenschutzgerechten Handhabung

der Mitteilungen an die Krankenkassen dar. Nach Mitteilung des MDK in Bayern ist mit der Einführung dieses EDV-Verfahrens "ISmed-Neu" etwa Januar 1999 zu rechnen. Künftig - so der MDK in Bayern - könne das Ergebnis der Begutachtung in der Abfolge des Gesamtgutachtens vorgezogen werden, so daß es jedenfalls technisch möglich ist, der Kasse nurmehr dieses Ergebnisblatt zukommen zu lassen.

Allerdings beklagt der MDK zu meiner Forderung nach Reduzierung der Ergebnismitteilungen an die Kasse, daß ihre Erfüllung die Einflußmöglichkeit eines einzelnen MDK, somit auch des MDK in Bayern, überschreitet:

Nach dem Erkenntnisstand der Datenschutzbeauftragten der Länder tendieren die Verbände der Krankenversicherungen nach wie vor dazu, daß die Krankenkassen - ungeachtet datenschutzrechtlicher Einwände - möglichst alle beim MDK verfügbaren Informationen auch selbst erhalten. Dies rührt daher, daß der MDK in den Augen den Krankenkassen eine nur unselbständig und stets im Auftrag der Kassen handelnde Einrichtung ist. Die Spitzenverbände der gesetzlichen Krankenversicherung nehmen die Ausgestaltung des Verfahrens uneingeschränkt für sich in Anspruch und bieten den MDK in den Ländern kaum Mitspracherechte. Eine differenzierte Vereinbarung über den tatsächlichen Umfang der Mitteilungspflicht gemäß § 277 SGB V im Hinblick auf "ISmed-Neu" bleibt im Rahmen der Richtlinien über die Zusammenarbeit der Krankenkassen mit den Medizinischen Diensten nach § 282 Satz 3 SGB V anzustreben. Ebenso wie der BfD werde ich mich weiterhin um eine Reduzierung der Mitteilungen des MDK an die Krankenkassen nach § 277 SGB V auf das "Ergebnis" bemühen; dies gilt in gleicher Weise für die vergleichbare Frage des zulässigen Umfangs der Ergebnismitteilung der MDK-Begutachtung zur Feststellung der Pflegebedürftigkeit an die Pflegekassen.

4.8.2 Fehlbelegungsprüfungen in Krankenhäusern nach § 17 a KHG durch den MDK

Nach § 17 a Abs. 2 Krankenhausfinanzierungsgesetz (KHG) wirken die Krankenkassen insbesondere durch gezielte Einschaltung des MDK darauf hin, daß Fehlbelegungen vermieden und bestehende Fehlbelegungen zügig abgebaut werden. Zu diesem Zweck darf der MDK Einsicht in die Krankenunterlagen nehmen. Aus datenschutzrechtlicher Sicht stellt sich somit die Frage, was unter einer "gezielten Einschaltung des MDK" als Voraussetzung seines Einsichtsrechts in die Krankenunterlagen zu verstehen ist. Wollte man diese Vorschrift ausschließlich auf Einzelfallprüfungen hinsichtlich bestimmter Versicherter beschränken, bei denen sich etwa aus der Krankenhausabrechnung Anhaltspunkte für eine Fehlbelegung ergeben haben, hätte es der speziellen Regelung in § 17 a Abs. 2 KHG nicht bedurft; solche Einzelfallprüfungen waren nämlich bereits vor Erlass des § 17 a KHG nach den §§ 275 Abs. 1 Nr. 1, 276 Abs. 4 SGB V zulässig. Daher kann m.E. eine "gezielte Einschaltung" durchaus auch hinsichtlich einzelner Fachabteilungen eines **Krankenhauses** gegeben sein.

Allerdings müssen für eine "gezielte Einschaltung des MDK" konkrete, nachvollziehbare Kriterien für den Anlaß einer Überprüfung des Krankenhauses sowie für Umfang, Art und Weise der Durchführung dieser Prüfung festgelegt sein. Hinsichtlich Umfang, Art und Weise der Prüfung könnte ich mir vorstellen, daß man die Entscheidungen über diese Durchführungsmodalitäten **im einzelnen** dem MDK als gegenüber den Krankenkassen fachkompetenterer Einrichtung überlassen darf; möglicherweise findet der MDK im Verlauf seiner Prüfung Anlässe, Fehlbelegungen in weiteren Abteilungen des Krankenhauses zu untersuchen. Gewisse Vorgaben der Krankenkasse, die einen inhaltlichen Zusammenhang zwischen der bei einem Krankenhaus festgestellten Auffälligkeit und der dort vorzunehmenden Fehlbelegungsprüfung aufweisen, also ein entsprechendes "Grundkonzept" für diese Prüfung, erachte ich aber als notwendig, andernfalls liegt keine "gezielte Einschaltung" mehr vor.

Wenn die eben genannten Anforderungen an das Grundkonzept im übrigen erfüllt sind, halte ich zur Fehlbelegungsprüfung grundsätzlich auch die Ziehung einer prozentualen Stichprobe von Patienten für zulässig. **Auswahllisten** (eventuell - je nach fachlicher Erforderlichkeit - mit Fall-

Nrn., Geburtsjahr, Aufnahme- und Entlassungstag, Hauptdiagnose sowie behandelnder KH-Abteilung bzw. -station), die Krankenhäuser dem MDK zur Vorbereitung der Stichprobenziehung übersenden, dürfen mangels Erforderlichkeit jedenfalls keine Patientennamen enthalten, da es auf die Identität dieser Personen für die Ziehung einer Stichprobe nicht ankommt. Außerdem dürfen in derartigen Listen nur solche Krankenhausfälle mitgeteilt werden, die der MDK auch in seine Stichprobe einbeziehen darf, also nicht etwa Fälle von am Prüfungsauftrag ggf. nicht beteiligten Krankenkassen, Fälle privatversicherter Personen oder Fälle von Sozialhilfeempfängern.

Soweit der MDK seinen Auftrag zur Fehlbelegungsprüfung nach Einsichtnahme in die Krankenunterlagen auch anhand anonymisierter oder pseudonymisierter Unterlagen weiter- und durchführen kann, sobald also die Verarbeitung personenbezogener Patientendaten ggf. nicht mehr erforderlich ist, hat der MDK die Verarbeitung, insbesondere Speicherung personenbezogener Daten zu unterlassen.

Prüfaufträge der Krankenkassen für **stichprobenhaft ausgewählte Krankenhäuser** erfüllen mangels "Grundkonzept" für eine Fehlbelegungsprüfung nicht die Anforderungen an eine "gezielte Einschaltung des MDK", ebensowenig "gezielt" ist eine **flächendeckende** allgemeine, einer Ausforschung gleichkommende Überprüfung von Krankenhäusern.

Obwohl es gesetzessystematisch nicht auf den ersten Blick ersichtlich ist, erhebt und verarbeitet der MDK auch bei Fehlbelegungsprüfungen i.S.d. **§ 17 a Abs. 2 KHG Sozialdaten**, weil diese Vorschrift im Zusammenhang mit den sonstigen Aufgaben und Befugnissen des MDK im SGB V auszulegen ist: Ich sehe in solchen Fehlbelegungsprüfungen nach § 17 a Abs. 2 KHG eine i.S.d. **§ 275 Abs. 4 SGB V** "andere als die in § 275 Abs. 1 bis 3 genannte Aufgabe" der Krankenkassen und ihrer Verbände, bei der sie im notwendigen Umfang den MDK zu Rate ziehen. Gegenüber § 276 Abs. 2 Satz 2 SGB V, wonach Sozialdaten bei Aufträgen nach § 275 Abs. 4 SGB V vor der Übermittlung an den MDK zu anonymisieren sind, ist § 17 a Abs. 2 Satz 2 KHG eine Spezialregelung, die den MDK bei Fehlbelegungsprüfungen nach Maßgabe der Erforderlichkeit zur Einsicht in personenbezogene Krankenunterlagen berechtigt.

4.8.3 Überprüfung von Krankenhaus-Abrechnungen durch den MDK im Auftrag der Krankenkassen

Seitens mehrerer Krankenhäuser wurde ich um Äußerung gebeten, ob bei entsprechender Anforderung im Einzelfall Patientenunterlagen an den MDK übersandt werden dürfen, damit dieser die Abrechnungsart (Fallpauschale, Sonderentgelt, Pflegesatz) überprüfen kann. Ich habe hierzu folgende Auffassung vertreten:

Grundsätzlich ist davon auszugehen, daß der Gesetzgeber die in § 301 SGB V enthaltenen Datenübermittlungen der Krankenhäuser an die Krankenkassen als in der Regel zur Abrechnung ausreichend ansieht und daß § 301 SGB V insoweit einen abschließenden Katalog darstellt, welche Angaben die Krankenhäuser zur Abrechnung von Krankenhausfällen **an die Krankenkassen** übermitteln dürfen bzw. müssen.

Aus diversen Quellen ist mir jedoch bekannt, daß die neue Bundespflegesatzverordnung mit ihren Änderungsverordnungen die Abrechnung von Krankenhausfällen sowohl für die abrechnenden Krankenhäuser als auch für die Krankenkassen erschwert hat. Die Einordnung von Diagnosen und Prozeduren in das komplizierte Vergütungssystem der Bundespflegesatzverordnung mit Fallpauschalen und Sonderentgelten sowie Abteilungs- und Basispflegesätzen ist auf seiten der Krankenkassen in manchen Fällen ohne Rückgriff auf medizinischen Sachverstand wohl nicht möglich, wie von Kassen- bzw. MDK-Seite - bislang unwiderlegt - vorgetragen wird. Die Krankenkassen sowie der MDK sind danach manchmal nicht in der Lage, allein aus dem Datensatz nach § 301 SGB V die Richtigkeit von Krankenhaus-Abrechnungen beurteilen zu können, so daß der MDK auf Unterlagen aus der Patientenakte wie etwa auf den ärztlichen Entlassungsbericht, den OP-Bericht etc. angewiesen sein kann, um z.B. überprüfen zu können, ob die sog. Hauptdiagnose des Krankenhauses als wesentliche Voraussetzung sowohl für die Behandlung als auch für die Einordnung in die Abrechnungssystematik der Bundespflegesatzverordnung vom Krankenhaus richtig gewählt wurde oder ob aus ganz bestimmten, definierten Bedingungen Fallpauschale und Sonderentgelte oder mehrere Sonderentgelte nebeneinander abgerechnet werden dürfen.

Angesichts dieser Situation erachte ich es nach derzeitigem Erkenntnisstand für zulässig, wenn

die Krankenkassen einzelne Krankenhaus-Abrechnungen auf der Grundlage des § 275 Abs. 1 Satz 1 Nr. 1 SGB V ("Prüfung von Voraussetzung, Art und Umfang der Leistung") dem MDK mit der Bitte um gutachtliche Stellungnahme vorlegen. Nicht für vereinbar mit § 275 Abs. 1 Satz 1 Nr. 1 SGB V halte ich jedoch flächendeckende und/oder stichprobenweise Prüfungen von Krankenhaus-Abrechnungen, etwa zu Präventionszwecken; vielmehr sind Begutachtungen durch den MDK nach § 275 Abs. 1 Satz 1 Nr. 1 SGB V lediglich einzelfallbezogen, d.h. patientenbezogen zulässig. Gerade auch bei der jeder Kostenübernahme vorausgehenden Prüfung des Umfangs der Leistungsverpflichtung durch die Krankenkasse kann sich an einzelnen Positionen in Krankenhaus-Abrechnungen zeigen, daß die MDK-Einschaltung "nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf" erforderlich ist und der MDK gegenüber der Krankenkasse "bei Erbringung von Leistungen, insbesondere zur Prüfung von Voraussetzung, Art und Umfang der Leistung" gutachtlich Stellung nehmen muß. Insoweit halte ich entsprechende Überprüfungen einzelner Krankenhaus-Abrechnungen durch den MDK und dabei seine Prüfungen von "Voraussetzung, Art und Umfang der Leistung" untrennbar miteinander verbunden.

Gemäß § 276 Abs. 2 Satz 1 2. Hs. SGB V sind die Leistungserbringer verpflichtet, Sozialdaten (hier: Patientendaten) auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist, die die Krankenkassen nach § 275 Abs. 1 bis 3 SGB V veranlaßt haben. Soweit die Leistungserbringer Patientendaten nach diesen Bestimmungen an den MDK übermitteln, liegt keine unbefugte Durchbrechung der ärztlichen Schweigepflicht vor. Sozialdaten/Patientendaten in diesem Sinne sind auch ausführliche medizinische Begründungen, die Inhalte der Krankenakte zusammenfassen.

Die Krankenhäuser dürfen personenbezogene Krankenunterlagen allerdings lediglich nach Maßgabe der Erforderlichkeit zur Überprüfung und nur so an den MDK weiterleiten, daß eine Kenntnisnahme vom Inhalt dieser Datenübermittlungen durch die Krankenkassen ausgeschlossen ist (§ 276 Abs. 2 Satz 1 2. Hs. SGB V), vgl. hierzu auch [Nr. 4.4.2](#) meines 17. Tätigkeitsberichts - 1996 -.

4.9 Rentenversicherung

Dialogverfahren der Rentenversicherungsträger zu Beratungszwecken

In meinem 17. Tätigkeitsbericht - 1996 - habe ich unter [Nr. 4.10](#) über die gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung und über meine Anforderungen an die technischen und organisatorischen Sicherungsmaßnahmen im Sinne von § 78 a SGB X berichtet. An diesem Dialogverfahren der Rentenversicherungsträger, bei dem der einzelne Versicherte die von ihm gewünschten Informationen über sein Versicherungsverhältnis und über bisher erworbene Anwartschaftsrechte auch bei einem anderen als dem nach den einschlägigen Organisations- und Kompetenzvorschriften für ihn zuständigen RV-Träger erhalten kann, nimmt mittlerweile auch die Bundesversicherungsanstalt für Angestellte teil.

Nach meinem Erkenntnisstand haben die RV-Träger in meinem Zuständigkeitsbereich das Dialogverfahren mit umfangreichen Sicherheitsvorkehrungen technischer und organisatorischer Art abgesichert. Der Verband Deutscher Rentenversicherungsträger (VDR) hat dem Bundesbeauftragten für den Datenschutz zugesagt, das Dialogverfahren Anfang 1999 um ein technisches Merkmal zu ergänzen, durch das die Anzeige des Versicherungskontos beim unzuständigen Rentenversicherungsträger auf Widerspruch des Versicherten hin unterbunden wird. Damit wird nun bundesweit eine Forderung erfüllt, die auch ich in meinem Zuständigkeitsbereich gegenüber den RV-Trägern erhoben habe. Da in der letzten Ausbaustufe des Dialogverfahrens davon auszugehen ist, daß voraussichtlich jeder RV-Träger technisch die Möglichkeit haben soll, bundesweit auf die Versicherungskonten aller Versicherten zugreifen zu können, hatte ich es für datenschutzrechtlich äußerst problematisch erachtet, wenn den Betroffenen keinerlei Einwirkungsmöglichkeit auf die bundesweite Abrufbarkeit ihrer Daten zu Beratungszwecken eingeräumt wird.

Schließlich sind von diesem flächendeckenden Verfahren zahlreiche Versicherte betroffen, die diesen Service aufgrund ihrer Selbsthaftigkeit niemals benötigen werden oder die eine solche weitreichende Abfragemöglichkeit, aus welchen Gründen auch immer (etwa, weil Verwandte bei einem RV-Träger beschäftigt sind ...), nicht wünschen: Da das Dialogverfahren als **Serviceleistung für die Versicherten** gedacht ist, hatte sich die Frage aufgedrängt, weshalb sich die Be-

troffenen nicht auch gegen die generelle technische Abrufbarkeit ihrer Daten entscheiden können sollten.

Wenn sich die Betroffenen also ihrerseits beim zuständigen RV-Träger (Kontoführer) melden und die externe Zugriffsmöglichkeit anderer RV-Träger auf ihre Daten ausdrücklich ablehnen, wird ab Anfang 1999 technisch unterbunden, daß externe RV-Träger zu Beratungszwecken auf das betreffende RV-Konto zugreifen.

Nach wie vor sehe ich es zu Dokumentations- und Kontrollzwecken für erforderlich an, daß der betroffene Versicherte und nicht lediglich der zuständige Mitarbeiter des RV-Trägers durch seine Unterschrift dokumentiert, daß die Anforderung des Versicherungskontos beim kontoführenden RV-Träger dem Wunsch des Versicherten gemäß zu seiner Beratung erfolgte. Ohne die Unterschrift des Betroffenen erscheinen mir stichprobenmäßige Kontrollen, daß für protokollierte Zugriffe ein Antrag vorliegt, im Hinblick auf die bundesweite Abrufbarkeit von Versichertenkonten nicht angemessen aussagekräftig. Solche schriftlichen Bestätigungen der Auskunft wünschenden Versicherten erfordern keinen nennenswerten Aufwand, wenn sie formularmäßig umgesetzt werden. Einzelne RV-Träger praktizieren diese Verfahrensweise bereits.

Darüberhinaus bereitete meine weitere Forderung, die Identitätsprüfung der Antragsteller, die in einer Beratungsstelle vorsprechen, **anhand eines Lichtbildausweises** vorzunehmen und dies zu dokumentieren, einzelnen RV-Trägern zunächst Akzeptanzprobleme. Es mag zwar grundsätzlich möglich sein, eine Identitätsprüfung auch anhand anderer Dokumente bzw. gezielter Fragen vorzunehmen, die nur der Versicherte selbst beantworten kann; zu Kontrollzwecken müßte dann aber vom Mitarbeiter der Auskunfts- und Beratungsstelle aufgezeichnet (und vom Betroffenen bestätigt) werden, wie die Identitätsprüfung des Antragstellers jeweils im einzelnen erfolgte. Demgegenüber dürfte die Identitätsprüfung durch Lichtbildausweis wesentlich einfacher sein.

Der Antragsteller wird diese Verfahrensweise akzeptieren, wenn ihm der Mitarbeiter des beratenden RV-Trägers erklärt, daß durch Vorlage des Lichtbildausweises sicher ausgeschlossen werden soll, daß der RV-Träger Dritten (etwa Gläubigern, Versicherungsvertretern usw.) unbefugt Auskunft erteilt. Diese datenschutzsichernden Maßnahmen erfolgen damit im Interesse und zur Sicherheit des Versicherten.

Ich stehe der Nutzung moderner EDV-Verfahren grundsätzlich positiv gegenüber. Je nachdem aber, wie flächendeckend solche EDV-Verfahren eingesetzt werden sollen und wie das Risiko von Verletzungen des Rechts auf informationelle Selbstbestimmung der Betroffenen einzustufen ist, müssen die Anwender solcher Verfahren den entstehenden Gefahren durch dementsprechend angemessene technische und organisatorische Sicherungsmaßnahmen begegnen. Schließlich enthalten die Rentenversicherungskonten sehr persönliche Sozialdaten wie insbesondere Angaben über erzielte Entgelte, Krankheits- und Arbeitslosigkeitszeiten, Zeiten verminderter Erwerbstätigkeit, Pfändungen usw.

5. Polizei

5.1 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren

- **allgemeine Kontrolle von Dateien und Karteien**, insbesondere des Kriminalaktennachweises (KAN), der Datei polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV), des Schengener Informationssystems (SIS), der Staatsschutzdatei Bayern (SDBY) sowie von Dateien zur Gefahrenabwehr und Strafverfolgung (sog. GAST-Dateien)
- **Überprüfung von Errichtungsanordnungen für polizeiliche Dateien** (Personen- und Fall-Auskunftsdatei - PFAD, System zur Verknüpfung von Gewaltverbrechen - VICLAS, Arbeitsdatei "Rauschgift", Datei "Pkw-Aufbrüche/Einbruchdiebstähle", sowie verschiedene GAST-Dateien)
- **Kontrolle von Datenerhebungsmaßnahmen**
- **Kontrolle von Datenübermittlungen**
- **Kontrolle von Abfragen polizeilicher Informationssysteme**
- **Kontrolle der Auskunftserteilung an Betroffene über Speicherungen in Dateien**

- **Mitwirkung an Gesetzen und Richtlinien**
- **Mitwirkung im Arbeitskreis Sicherheit**
- **sonstige Bürgereingaben**

Ein- und mehrtägige Prüfungen habe ich beim Bayerischen Landeskriminalamt, verschiedenen Polizeipräsidien, Polizei- und Kriminalpolizeidirektionen und deren nachgeordneten Dienststellen vorgenommen.

5.2 Ergebnisse meiner Prüfungen und Bewertung von Grundsatzthemen

Bei meinen Prüfungen und aufgrund von Bürgereingaben habe ich festgestellt, daß datenschutzrechtliche Verstöße bei der bayerischen Polizei z.T. auf Fehlleistungen einzelner Bediensteter beruhen, aber auch auf systemimmanente Mängel zurückzuführen sind. Die wesentlichen Fehler und Mängel führe ich in nachstehender Darstellung auf. Diese Feststellungen wären aber ohne den Hinweis unvollständig, daß unsere Prüfungen in weiten Bereichen auch keine datenschutzrechtlichen Mängel ergeben haben.

5.3 Allgemeine Kontrolle von Dateien und Karteien

5.3.1 Kriminalaktennachweis (KAN)

Der Kriminalaktennachweis der Bayerischen Polizei (KAN) ist ein landesweites polizeiliches elektronisches Informationssystem und wesentlicher Bestandteil des Dateisystems "Personen- und Fall-Auskunftsdatei-Bayern" (PFAD). Sein Hauptzweck ist die Erteilung einer aktuellen Kurzauskunft über die in Kriminalakten enthaltenen Unterlagen zu Straftaten, schwerwiegenden Ordnungswidrigkeiten sowie über Unterlagen und Hinweise, die der Gefahrenabwehr oder vorbeugenden Kriminalitätsbekämpfung dienen. Zugangs- bzw. abfrageberechtigt sind in der Regel alle bayerischen Polizeivollzugsbeamten sowie Angestellte der Polizei, wenn diesen bestimmte Aufgaben besonders übertragen wurden. Der Zugriff wird aufgaben- und funktionsbezogen im Rahmen eines Ebenen- und Zugriffsschutzkonzepts durch abgestufte Berechtigungen festgelegt.

Die Rechtsgrundlage für die Speicherung personenbezogener Daten im Kriminalaktennachweis (KAN) ist Art. 38 Polizeiaufgabengesetz (PAG). Nach dieser Vorschrift kann die Polizei personenbezogene Daten in Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Sie kann insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern, verändern und nutzen, "soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Entfällt der der Speicherung zugrundeliegende Verdacht, sind die Daten zu löschen."

Im Oktober 1997 wurde der Öffentlichkeit wie auch mir durch einen Pressebericht bekannt, daß personenbezogene Daten auf unzulässige Weise durch die Polizei an die Presse übermittelt worden waren. Wie sich herausstellte, war die weitere Speicherung dieser Daten unzulässig, weil der Tatverdacht gegen die betroffene Person entfallen war und dies der Polizei von der Staatsanwaltschaft auch mitgeteilt worden war. Die vorgeschriebene Löschung war jedoch unterblieben. Dies habe ich beanstandet.

Dem Pressebericht war auch zu entnehmen, daß im Kriminalaktennachweis der Bayerischen Polizei 800.000 Personen gespeichert sein sollen.

Den Sachverhalt und die m.E. sehr hohe berichtete Anzahl der Personendatensätze im bayerischen KAN habe ich zum Anlaß genommen, eine Querschnittsprüfung der Speicherpraxis der bayerischen Polizei im Kriminalaktennachweis vorzunehmen. Gleichzeitig habe ich die Anzahl der Personendatensätze in vergleichbaren polizeilichen Informationssystemen der anderen deutschen Länder und des Bundes erhoben.

Ziel meiner Prüfung war es, festzustellen, ob das System der Speicherung personenbezogener Daten und deren Überprüfung nach Abschluß des strafrechtlichen Verfahrens datenschutzgerechte Ergebnisse gewährleistet, insbesondere sicherstellt, daß die gesetzlichen Speichervoraussetzungen vorliegen. Schwerpunkt meiner Prüfung war, ob der für die Speicherung erforderliche Tatverdacht nach Verfahrenseinstellung gem. § 170 Abs. 2 StPO fortbestand und ob die Polizei

von der Staatsanwaltschaft bei Wegfall des Tatverdachts entsprechend unterrichtet wurde.

Geprüft habe ich 211 Datenspeicherungen bei verschiedenen bayerischen Polizeidienststellen und 4 Datenspeicherungen, die mir aufgrund von Eingaben bekannt geworden waren. Die Prüfung ergab folgendes:

- Statt der in der Pressemeldung genannten 800.000 Personendatensätze waren im Kriminalaktennachweis der bayerischen Polizei tatsächlich 1,31 Millionen Personendatensätze gespeichert. **Im Vergleich entspricht** das 10,8% der Wohnbevölkerung Bayerns und liegt damit weit über dem Durchschnitt von 5,93 % in den Ländern. Nach Berlin (16,5%) bedeutet das die prozentual zweithöchste Speicherung in der Bundesrepublik Deutschland.
- Von den 215 geprüften Fällen waren 149 im KAN bzw. in der Kriminalakte mit personenbezogenen Daten gespeichert. Bei 16 der gespeicherten Fälle (10,7 %) war der Tatverdacht entfallen bzw. konnte m.E. kein Tatverdacht **von ausreichender Substanz** festgestellt werden, der eine Weiterspeicherung trotz Einstellung des Strafverfahrens durch die Staatsanwaltschaft gerechtfertigt hätte.
- In 5 der obengenannten 16 Fälle unterließ die Staatsanwaltschaft die auch nach Auffassung des Staatsministeriums der Justiz gebotene Mitteilung, daß der Tatverdacht entfallen ist. In 2 weiteren Fällen führte die Mitteilung bei der Polizei nicht zur Löschung. Auch in den restlichen 9 Fällen war ein Tatverdacht **von ausreichender Substanz** nicht mehr gegeben war. Die Speicherungen blieben gleichwohl bestehen.
- In etwa 30 von 149 Fällen fehlte die Mitteilung der Staatsanwaltschaft über den Verfahrensausgang in der Kriminalakte der Polizei, bzw. war das Formblatt mit dem die Mitteilung erfolgt, nicht ausgefüllt. Das sind etwa 20 % der geprüften Fälle.

Das Ergebnis meiner Prüfung bewerte ich wie folgt:

5.3.1.1 Speicherung nach Verfahrenseinstellung

Im Vergleich zur Mehrzahl der anderen deutschen Länder, insbesondere zu allen Flächenländern, ist die Anzahl der im bayerischen KAN gespeicherten Personendatensätze hoch, auch wenn dabei zu berücksichtigen ist, daß Faktoren, wie z.B. die jeweilige Kriminalitäts- und Aufklärungsquote (eine hohe Aufklärungsquote bewirkt zwangsläufig eine höhere Anzahl von Datensätzen Tatverdächtiger) und der Anteil Bayerns an Außengrenzen und der damit verbundenen erhöhten Speicherung ausländischer Tatverdächtiger eine Rolle spielen. Andererseits findet in Bayern gemäß Nr. 1.2 der Anlage 3 zu den PpS-Richtlinien in der Regel keine polizeiliche Prüfung des Fortbestehens des Tatverdachts nach Verfahrenseinstellungen gem. § 170 Abs. 2 StPO statt, was ich wesentlich mitursächlich für die hohe Zahl der KAN-Speicherungen ansehe. Diese Richtlinien war zwar seinerzeit mit dem damaligen Landesbeauftragten für den Datenschutz abgestimmt. Die Ergebnisse meiner datenschutzrechtlichen Querschnittsprüfung haben mir aber gezeigt, daß dieses Verfahren nicht geeignet ist, die Einhaltung der gesetzlichen Speichervoraussetzungen - Fortbestehen eines Tatverdachts - zu gewährleisten.

Die Staatsanwaltschaft ist zwar gehalten, der Polizei den Verfahrensausgang mitzuteilen, sie prüft aber nicht, ob ein für die polizeiliche Speicherung erforderliche Tatverdacht von ausreichender Substanz noch gegeben ist. Diese Prüfung obliegt der Polizei als speichernde Stelle.

Die fehlende Prüfung hat zur Folge, daß nach Verfahrenseinstellung auch Fälle gespeichert werden, bei denen ein die weitere Speicherung rechtfertigender Tatverdacht von Substanz nicht mehr gegeben ist. Durch eine solche Speicherung kann der Betroffene erheblich belastet werden, sei es durch intensive polizeiliche Kontrollen im Einzelfall oder durch die Gefahr, unbegründet in den Kreis der Verdächtigen einer Straftat mit einbezogen zu werden. Auch können solche Speicherungen anderen öffentlichen Stellen, z.B. im Rahmen von Zuverlässigkeitsprüfungen, mitgeteilt werden, was höchst nachteilige Folgen für den Betroffenen haben kann.

Hier besteht ein gravierendes Handlungsdefizit seitens der Polizei.

Der Staatsminister des Innern hat eine Überprüfung der Richtlinien für die Führung polizeilicher personenbezogener Sammlungen zugesagt.

Verbessert werden sollte auch die meinen Feststellungen zufolge lückenhafte Unterrichtung der Polizei über den Verfahrensausgang durch die Staatsanwaltschaften. Das Justizministerium hat die Staatsanwaltschaften auf die Bedeutung und die Notwendigkeit der Mitteilung über den Verfahrensausgang und ggf. des Wegfalls des Tatverdachts hingewiesen.

Darüberhinaus sollte die Polizei von der Staatsanwaltschaft in jedem Fall, in dem der Tatverdacht entfallen ist, hierüber informiert werden, damit sie der gesetzlichen Lösungsverpflichtung nachkommen kann. Die Anordnung einer solchen Mitteilung an die Polizei darf nicht, wie bisher, davon abhängig gemacht werden, ob der Beschuldigte vernommen wurde oder ob er ein besonderes Interesse an der Mitteilung der Einstellung hat.

Ferner habe ich auch darauf hingewiesen, daß der Beschuldigte in Fällen, in denen er keine Kenntnis vom Verfahren hat, auch nicht mit der Möglichkeit der Speicherung in polizeilichen Dateien rechnet. Um seine grundsätzlich bestehenden Rechte auf Auskunft, ggf. Berichtigung, Sperrung oder Löschung gegenüber der Polizei wahrnehmen zu können, halte ich es für erforderlich, daß er über die Einstellung des Verfahrens informiert wird. Der Beschuldigte hat - selbst wenn er völlig unschuldig in Verdacht geraten ist - ohne entsprechende Mitteilung keine Chance, auf eine Löschung in polizeilichen Dateien hinzuwirken. Ich habe daher gegenüber dem Staatsministerium der Justiz ausgeführt, daß das Gesetz verfassungskonform dahingehend auszulegen ist, daß auch jeder Beschuldigte, der vom Verfahren keine Kenntnis hat, über die Einstellung zu informieren ist.

Das Justizministerium hat mir mitgeteilt, daß meine beiden letztgenannten Forderungen mit den Leitern der Staatsanwaltschaften besprochen und ich über das Ergebnis unterrichtet werde.

Weitere Forderungen an das Staatsministerium des Innern zur Reduzierung der hohen Anzahl von KAN-Speicherungen sind in den nachfolgenden Beiträgen erläutert.

5.3.1.2 Speicherungsfristen

Nach dem Polizeiaufgabengesetz (PAG) ist die Dauer der Speicherung auf das erforderliche Maß zu beschränken. Für automatisierte Dateien sind Termine festzulegen, an denen spätestens überprüft werden muß, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine). Dabei sind Speicherungszweck sowie Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen. Die festzulegenden Prüftermine und Aufbewahrungsfristen dürfen bei Erwachsenen 10 Jahre, bei Jugendlichen 5 Jahre und bei Kindern 2 Jahre nicht überschreiten. Diese Fristen sind Höchstfristen und nicht etwa Regelfristen, wie in der Vollzugsbekanntmachung zum Polizeiaufgabengesetz festgelegt wird. Dies hat der Bayerische Verwaltungsgerichtshof in seinem Urteil vom 04.06.1996 entschieden. Dem entspricht die polizeiliche Speicherungspraxis nicht, die sich nach meinen Erkenntnissen grundsätzlich an der Höchstfrist orientiert. Diese generalisierende und zu wenig differenzierte Vergabe der Fristen halte ich deshalb für unzulässig. Die von mir angeforderte Stellungnahme des Staatsministeriums des Innern hierzu steht noch aus.

5.3.1.3 Automatische Fristenverlängerung

Eine weitere Ursache für die hohe Anzahl von KAN-Speicherungen sehe ich in der polizeilichen Praxis, eine Speicherung nach Ablauf der Speicherungsfrist dann nicht zu löschen, wenn eine oder mehrere weitere Speicherungen zur selben Person mit längerer Speicherungsfrist erfaßt sind oder während des Laufs der Erstspeicherung erfaßt werden. Nach dieser Praxis ist für die Speicherdauer nicht die für einen Vorgang vergebene Einzelfrist maßgebend, sondern beim Vorhandensein oder Hinzutreten weiterer Speicherungen die längste vergebene Frist. So verlängert sich z.B. die Speicherungsfrist für einen Vorgang, der nach 10 Jahren kurz vor der Löschung steht, bei der Speicherung eines neuen Vorgangs um weitere 10 Jahre auf insgesamt 20 Jahre, wenn der hinzukommende Vorgang seinerseits mit einer Speicherdauer von 10 Jahren erfaßt wird. Der Bayerische Verwaltungsgerichtshof hat in seinem Urteil vom 4. Juni 1996 unter Hinweis, daß die Formulierung in Art. 38 Abs. 2 Satz 5 PAG diese Rechtsfolge nicht trage, dazu ausgeführt, daß die für jedes einzelne Ereignis vergebene Speicherungsfrist für sich allein zu betrachten ist. Dies bedeutet eine getrennte Berechnung des Fristlaufs für jedes einzelne Verfah-

ren, so daß die jeweilige Speicherung nach Ablauf der individuellen Frist zu löschen und der Vorgang zu vernichten ist.

Die Stellungnahme des Staatsministeriums des Innern , das ich auf die Problematik ausdrücklich hingewiesen habe, steht noch aus.

5.3.1.4 Vergabe von personenbezogenen Hinweisen (PHW)

Zu Datenspeicherungen im Kriminalaktennachweis (KAN) können zusätzlich sogenannte personenbezogene Hinweise (PHW) vergeben werden. Sie dienen der Eigensicherung einschreitender Beamter, der Einleitung gezielter Fahndungsmaßnahmen, der Unterstützung von Ermittlungen und dem Schutze Betroffener bei polizeilichen Maßnahmen. Die Art der personenbezogenen Hinweise und deren Speichervoraussetzungen sind in der Errichtungsanordnung PFAD (vgl. [17. Tätigkeitsbericht Nr. 5.7](#)) abschließend definiert. Die Speicherung von personenbezogenen Hinweisen habe ich bei zwei Polizeidirektionen geprüft. Insbesondere bei zwei Arten personenbezogener Hinweise habe ich datenschutzrechtliche Defizite festgestellt:

- Personenbezogene Hinweis ANST (Ansteckungsgefahr)

Dieser personenbezogene Hinweis (PHW) darf nach der Errichtungsanordnung nur vergeben werden, wenn der Betroffene unter einer nach § 3 des Bundesseuchengesetzes meldepflichtigen Krankheit leidet oder wenn ein **ärztlicher Hinweis** vorliegt, daß er gem. § 2 des Gesetzes krank, krankheitsverdächtig, ansteckungsverdächtig, Ausscheider oder ausscheidungsverdächtig ist und eine Ansteckung eine schwerwiegende Gesundheitsgefährdung bedeuten würde. Der Hinweis muß vom Arzt zumindest mündlich vorliegen oder von einer öffentlichen Stelle schriftlich oder mündlich mitgeteilt werden, wobei bei mündlicher Mitteilung umgehend eine schriftliche Bestätigung einzuholen ist, oder die Hinweise müssen auf "konkreten, glaubhaften Angaben des Betroffenen oder naher Angehöriger" beruhen. Der Hinweisgeber ist in der Kriminalakte zu dokumentieren (wer, wann, was).

Wegen der Möglichkeit einer Speicherung des PHW aufgrund "konkreter glaubhafter Angaben naher Angehöriger", habe ich mich an das Staatsministerium des Innern gewandt. Die Speicherung einer Person als "ansteckungsgefährlich" stellt einen gravierenden Eingriff in das Persönlichkeitsrecht des Betroffenen dar. Beruht die Datenspeicherung ausschließlich auf den Angaben Dritter, sind die Daten so lange ungesichert, bis deren Richtigkeit durch die Angaben des Betroffenen oder durch ein ärztliches Gutachten bestätigt werden. So könnte beispielsweise ein naher Angehöriger - auch dieser Begriff ist auslegungsfähig - aus persönlichen Gründen falsche Angaben über die Ansteckungsgefahr eines Betroffenen machen. Dem Betroffenen sollte deshalb in diesen Fällen Gelegenheit gegeben werden, der Speicherung entgegenzutreten zu können.

Das Staatsministerium des Innern hat diese Forderung abgelehnt.

Die Dauer der zulässigen Speicherung des personenbezogenen Hinweises ANST beträgt nach der Errichtungsanordnung PFAD zwei Jahre. Bei meiner Prüfung einer Polizeidirektion habe ich festgestellt, daß die Speicherungen in mehreren Fällen verlängert wurden, obwohl keine neuen Erkenntnisse vorlagen, die die Annahme von Ansteckungsgefahr positiv belegt hätten. Nach meiner Auffassung ist keine Verlängerung der Speicherung zulässig, sondern nur eine Neuvergabe mit erneuter Prüfung des Vorliegens der Vergabevoraussetzungen. Die Unkenntnis über den Krankheitsverlauf ist für eine erneute Speicherung grundsätzlich nicht ausreichend. Auch in diesem Fall ist die Speicherung regelmäßig nach zwei Jahren zu löschen. Die unzulässig verlängerten Speicherungen wurden auf meine Aufforderung von der Polizei gelöscht. In zwei Fällen hielt ich die Neuvergabe des personenbezogenen Hinweises ausnahmsweise für vertretbar, da die beiden Personen untergetaucht zu sein schienen und die Umstände dafür sprachen, daß sie sich bislang keiner ärztlichen Behandlung unterzogen hatten oder unterziehen werden.

Bei beiden Polizeidirektionen habe ich bei meiner Prüfung festgestellt, daß einige Speicherungen des personenbezogenen Hinweises ANST erfolgt sind, obwohl weder ein Vermerk über eine ärztliche mündliche Mitteilung noch eine entsprechende schriftliche Mitteilung oder Bestätigung einer öffentlichen Stelle vorlag. Die Polizei wurde von mir

aufgefordert, die fehlenden Mitteilungen unverzüglich einzuholen und diese zu dokumentieren oder die personenbezogenen Hinweise zu löschen. Eine Polizeidirektion hat daraufhin die erforderlichen ärztlichen Mitteilungen erholt, bei der anderen Polizeidirektion steht das Ergebnis noch aus.

- Personenbezogener Hinweis GEKR (Geisteskrank)

Der personenbezogene Hinweis (PHW) GEKR darf nach der Errichtungsanordnung nur erfaßt werden, wenn ärztlich festgestellt ist, daß der Betroffene an einer Geisteskrankheit leidet. Dazu genügt die mündliche Aussage des Arztes oder die mündliche Übermittlung einer solchen ärztlichen Feststellung durch eine Behörde, die jedoch umgehend schriftlich zu bestätigen ist. Die mündliche Übermittlung ist in der Kriminalakte zu dokumentieren (wer, wann und was). Auch bei meiner Überprüfung dieser Datenspeicherungen habe ich festgestellt, daß bei drei von zehn Datensätzen keine ärztliche Feststellung der Geisteskrankheit dokumentiert war. Die Polizeidirektion wurde aufgefordert, diese unverzüglich nachzuholen oder bei fehlenden Voraussetzungen die personenbezogenen Hinweise unverzüglich zu löschen. Das Ergebnis steht noch aus.

5.3.1.5 Speicherung von Fällen geringerer Bedeutung

Gem. Art 38 Abs. 2 Satz 4 PAG sind in Fällen von geringerer Bedeutung kürzere Fristen festzusetzen. Das Staatsministerium des Innern hat der Polizei Regelbeispiele für Fälle geringerer Bedeutung in Richtlinien vorgegeben. Hiernach handelt es sich um einzelne fahrlässig begangene Straftaten, Privatklagedelikte, Ordnungswidrigkeiten und ähnliches. Die Regelspeichungsfrist für diese Delikte ist auf 5 Jahre festgelegt. Sie dürfen als alleinige Unterlage nicht im KAN nachgewiesen werden, sondern nur in der Datei PSV (vgl. [Nr. 5.3.2](#)). Die einschränkende Aufzählung von Regelbeispielen von Fällen geringerer Bedeutung, an der sich die polizeiliche Praxis ausrichtet, und die pauschale Speicherung solcher Fälle für 5 Jahre wird der gesetzlichen Regelung nicht gerecht. Bei allen Straftatbeständen (ausgenommen schwere und schwerste Straftaten) können Fälle geringerer Bedeutung in Betracht kommen. Dies ist jeweils im Rahmen einer Ein-

zelfallprüfung unter Berücksichtigung relevanter Entscheidungskriterien, wie z.B. Bedeutung der Tat, Schuldgehalt, Wiederholungsgefahr, Motiv etc. von der Polizei zu beurteilen.

Auch hierzu steht die Stellungnahme des Staatsministeriums des Innern noch aus.

5.3.1.6 Sperren von Daten

Im Rahmen meiner datenschutzrechtlichen Prüfung von Datenspeicherungen der Polizei aufgrund einer Bürgereingabe stellte ich fest, daß ein Polizeipräsidium die gespeicherten Daten aufgrund meiner Anfrage gelöscht hatte. Nach den Angaben des von der Speicherung betroffenen Bürgers und nach meinen Erkenntnissen gab es Anhaltspunkte dafür, daß die Speicherungen bis zum Zeitpunkt der Löschung unzulässig gewesen sein könnten. Durch die Löschung der Daten und die Vernichtung der Unterlagen war eine Prüfung der Zulässigkeit der früheren Speicherungen nur mehr bedingt möglich, so daß ich letztendlich nicht feststellen konnte, ob ein datenschutzrechtlicher Verstoß vorgelegen hatte. Diese vorzeitige Löschung war unzulässig. Gem. Art. 45 Abs. 2 PAG sind in Dateien suchfähig gespeicherte personenbezogene Daten zwar zu löschen und die zu dem Betroffenen geführten Akten zu vernichten, wenn ihre Speicherung unzulässig war. Gem. Art. 45 Abs. 3 PAG hat die Löschung und Vernichtung jedoch zu unterbleiben, wenn Grund zu der Annahme besteht, daß schutzwürdige Interessen des Betroffenen beeinträchtigt würden. In diesen Fällen sind die Daten zu sperren und mit einem Sperrvermerk zu versehen. Die schutzwürdigen Interessen des Betroffenen waren in diesem Fall beeinträchtigt, weil er gegen die möglicherweise unzulässige Speicherung im Kriminalaktennachweis vorgehen wollte, und dazu u.a. den Landesbeauftragten für den Datenschutz um Überprüfung gebeten hatte. Deshalb hätten die Daten wie vorgeschrieben nicht gelöscht sondern für den allgemeinen Zugriff gesperrt werden müssen, bis meine datenschutzrechtliche Prüfung sowie die evtl. Inanspruchnahme von Rechtsschutz seitens des Betroffenen abgeschlossen gewesen wären. Es bedarf deshalb vor Löschung der Daten grundsätzlich einer sorgfältigen Prüfung im Hinblick auf offenkundige schutzwürdige Interessen des Betroffenen, insbesondere wenn sich sein Antrag auf Auskunft beschränkt und nicht auch ausdrücklich die Löschung seiner Daten zum Gegenstand hat. Die Polizei teilte mir mit, daß eine Sperrung von Daten im Kriminalaktennachweis technisch nicht möglich sei, so daß nur die Löschung bzw. Weiterspeicherung in Betracht komme. Ich ha-

be daraufhin das Staatsministerium des Innern aufgefordert, die entsprechende technische Möglichkeit zu schaffen, um den gesetzlichen Vorgaben für eine Sperrung entsprechen zu können. Das Staatsministerium des Innern hat mir mitgeteilt, daß das Landeskriminalamt mit der unverzüglichen technischen Umsetzung der Möglichkeit der Sperrung von KAN-Daten beauftragt wurde.

5.3.1.7 Verlängerte Speicherungsfrist bei Sexualstraftätern

Vor dem Hintergrund der in jüngerer Zeit verstärkten Medienberichterstattung über Sexualmorde an Kindern hat das Staatsministerium des Innern eine Anordnung zur Verlängerung der Aufbewahrungsfristen personenbezogener Sammlungen der Polizei im Zusammenhang mit Sexualstraftaten und Straftaten mit sexuellem Hintergrund getroffen. Dabei ist in Abänderung zur bisherigen Nr. 38.6 der Vollzugsbekanntmachung zum PAG eine regelmäßige Fristverlängerung für Sexualdelikte festgelegt worden. Im einzelnen wurde angeordnet, daß bei Beschuldigten oder Tatverdächtigen einer Sexualstraftat oder anderer Gewaltdelikte mit sexuellem Hintergrund die in Art. 36 Abs. 1 PAG genannten Prognosekriterien (die gemäß Art. 38 Abs. 3 PAG die Festlegung einer längeren Aufbewahrungsfrist für die gespeicherten Daten ermöglichen) in der Regel erfüllt seien. Die Aussonderungsprüffrist beträgt in der Regel 20 Jahre.

Gegen die Verlängerung der Aufbewahrungszeiten auf 20 Jahre habe ich keine grundsätzlichen Bedenken geäußert. Im Rahmen eines umfangreichen Meinungsaustausches mit dem Innenministerium habe ich jedoch in Einzelpunkten eine - wie ich meine - datenschutzgerechte Ausgestaltung der neuen Vorschrift erreicht. Diese sieht nunmehr eine differenzierende Regelung für Kinder, Jugendliche und Erwachsene vor. Aus dem Bereich der Sexualstraftaten, die zu einer verlängerten Speicherdauer berechtigen, wurden Straftatbestände wie z.B. die Verbreitung pornographischer Schriften nach § 184 StGB oder jugendgefährdende Prostitution gemäß § 184 b StGB, die jeweils nur Freiheitsstrafe bis zu einem Jahr vorsehen, ausgenommen. Schließlich konnte erreicht werden, daß von der Regelung neben den eigentlichen Sexualdelikten nicht alle Straftaten mit sexuellem Hintergrund, sondern nur Gewaltdelikte erfaßt werden. Hierdurch wird eine ausufernde Verlängerung der Aufbewahrungsfristen vermieden.

5.3.2 Datei polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)

Die Datei PSV ist ein elektronisches Datenverarbeitungssystem, das in erster Linie regional begrenzt bei den sog. Basisdienststellen, insbesondere bei den Polizeiinspektionen geführt wird. Mit ihr wurden die dort vormals manuell geführten Anzeigetagebücher und Neuigkeitsbögen abgelöst. Sie dient insbesondere dem Nachweis und dem Auffinden des zu einem polizeilich relevanten Ereignis angefallenen Schriftverkehrs für einen angemessenen Zeitraum, der zeitlich befristeten Dokumentation polizeilicher Maßnahmen, der Information der Polizeibeamten über die in ihrem Zuständigkeitsbereich angefallenen Ereignisse - insbesondere im Hinblick auf den durch den Schichtbetrieb bedingten fortlaufenden Wechsel der Beamten - und ist Grundlage für die Bearbeitung von Beschwerden, Eingaben, Anträgen und Anfragen.

Erfasst werden insbesondere auch bestimmte Straftaten und Ordnungswidrigkeiten, die als "Fälle geringerer Bedeutung" (vgl. [Nr. 5.3.1.5](#)) im Kriminalaktennachweis (KAN) nicht gespeichert werden dürfen.

In der Datei PSV werden die Eckdaten zu einem polizeilich relevanten Ereignis erfasst, wie z.B. das Aktenzeichen, Bezeichnung des Ereignisses, Ereignisort und -zeit sowie die daran beteiligten Personen. Zum Zwecke der Vorgangsverwaltung und Dokumentation beträgt die regelmäßige Speicherdauer 5 Jahre.

5.3.2.1 Personenkategorien in der Datei PSV

In der Datei PSV werden die Personalien von den an einem Ereignis beteiligten Personen in zwei verschiedenen Personenkategorien erfasst. Die Personenkategorie "B" bezeichnet Beschuldigte, Tatverdächtige, Beteiligte an einer Ordnungswidrigkeit oder Betroffene polizeilicher Maßnahmen. Die Kategorie "Z" bezeichnet Zeugen und ist in weitere Kategorien, wie Geschädigte, Mit-teiler, Anzeigerstatter usw. untergliedert.

Die Erfassung eines Betroffenen unter der Kategorie "B" ist m.E. nur zulässig, soweit der o.g. Status tatsächlich vorliegt. Dies ist insbesondere dann nicht mehr der Fall, wenn sich aufgrund der Mitteilung des Verfahrensausgangs durch die Staatsanwaltschaft oder aus sonstigen Gründen ergeben hat, daß der Tatverdacht gegen einen Beschuldigten, Tatverdächtigen oder Betroffenen entfallen ist, deshalb auch ggf. vorhandene Speicherungen im Kriminalaktennachweis (KAN) zu löschen sind (vgl. [5.3.1](#)). Mit der Weiterspeicherung einer nunmehr unverdächtigen Person unter der "B"-Kategorie (Beschuldiger etc.) wird der Betroffene in unzumutbarer und unzulässiger Weise belastet, auch wenn die Speicherungen insbesondere nur internen Zwecken dient, sie sich aber im künftigen Verhalten der Polizei gegenüber dem Betroffenen negativ auswirken kann. Bei meiner Prüfung verschiedener Polizeidienststellen habe ich festgestellt, daß die vorgeschriebene Umschreibung von "B" auf "Z"-Personalie in zahlreichen Fällen nicht erfolgt ist. Die Verpflichtung ist in der für den Kriminalaktennachweis (KAN) und die Datei PSV ergangenen Errichtungsanordnung PFAD (vgl. [17. Tätigkeitsbericht Nr. 5.7](#)) festgelegt, die von der Polizei zu beachten ist. Auf meine Feststellungen habe ich die betroffenen Polizeidienststellen hingewiesen und zur Beachtung aufgefordert.

5.3.2.2 Schlagwortvergabe in der Datei PSV

In der Datei PSV können zu einem erfaßten Ereignis ein oder mehrere Schlagworte vergeben werden. Diese dienen der Polizei als zusätzlicher Hinweis auf die Art des Ereignisses oder als zusätzliche Information zu den erfaßten Personen für künftiges Einschreiten und als zusätzliches Recherchekriterium. Etwa 200 Schlagworte stehen zur Verfügung. Bei einer Polizeidirektion habe ich überprüft ob verschiedene von mir ausgewählte Schlagworte korrekt, insbesondere zutreffend vergeben wurden. Bei meiner Überprüfung der Vergabe des Schlagwortes AFPE (Auf-fällige Person) habe ich festgestellt, daß bei 5 von 10 Speicherungen das Schlagwort unzutreffend vergeben wurde. Die offizielle Definition des Schlagworts lautet: "Feststellungen im Rahmen der vorbeugenden Verbrechensbekämpfung ohne konkreten Tatverdacht". Das Schlagwort wurde u.a. aber vergeben, zu einer Frau, die aufgrund einer Bauchspeicheldrüsenerkrankung einen Schwächeanfall erlitten hatte, zu zwei betrunkenen Personen, die beide für kurze Zeit in polizeilichem Gewahrsam waren und zu zwei Personen, die einen Suizidversuch unternommen

hatten.

Nachdem trotz internen Gebrauchs der Datei PSV eine Belastung der Gespeicherten durch die Eintragung "Auffällige Person" zu befürchten ist, insbesondere bei deren erneuten Kontakten mit der Polizei, halte ich es für unbedingt erforderlich, die entsprechenden Schlagworte nur anhand der offiziellen Definition bei zutreffenden Sachverhalten zu vergeben. Bei meiner Prüfung stellte ich jedoch erhebliche Defizite bei der Kenntnis der Bedeutung verschiedener Schlagworte fest. Die betroffene Polizeidirektion hat auf meine Aufforderung entsprechende Schulungsmaßnahmen zum Ausgleich dieser Defizite vorgenommen und die unzutreffenden Speicherungen berichtigt.

5.3.3. Schengener Informationssystem (SIS)

Aufgrund des Schengener Übereinkommens und des Durchführungsübereinkommens (SDÜ) hierzu wurde durch die Aufhebung der Kontrollen an den Binnengrenzen der Vertragsparteien und die Einführung des Grundsatzes der einmaligen Kontrolle bei der Einreise in den Schengener Raum als Ausgleichsmaßnahmen u.a. das Schengener Informationssystem (SIS) eingeführt. Von den Vertragsparteien werden u.a. Daten zu Personen gespeichert, die von der Polizei gesucht oder überwacht werden, vermißte Personen oder Personen, die in Gewahrsam zu nehmen sind, insbesondere Minderjährige sowie Personen, denen die Einreise in das Schengener Hoheitsgebiet zu verweigern ist oder, deren Identität mißbräuchlich von anderen Personen verwendet wird. In Bayern ist das SIS über das Informationssystem der Bayerischen Polizei (IBP) erschließbar. So können über dieses System sowohl der Kriminalaktennachweis (KAN) wie auch das Schengener Informationssystem (SIS) abgerufen werden. Die Voraussetzungen für die Speicherung der personenbezogenen Daten sind im Schengener Durchführungsübereinkommen (SDÜ) geregelt. Bei meiner Überprüfung einer Datenspeicherung im SIS aufgrund einer Bürgeringabe habe ich festgestellt, daß die Speicherung der Ausschreibung des Betroffenen zur Einreiseverweigerung den Voraussetzungen des SDÜ bezüglich der Dauer des illegalen Aufenthalts nicht entsprach. Das betreffende Polizeipräsidium hat die Speicherung auf meine Aufforderung hin unverzüglich gelöscht. Die betroffenen Polizeidienststellen wurden vom Polizeipräsidium

auf den Mangel hingewiesen und zur künftigen Beachtung angehalten.

5.3.4 Weltwirtschaftsgipfel 1992

Bereits in meinen letzten Tätigkeitsberichten (vgl. zuletzt meinen [17. Tätigkeitsbericht Nr. 5.4.1](#)) hatte ich von den Ermittlungsverfahren im Zusammenhang mit den Vorkommnissen bei der Begrüßungszeremonie zum Weltwirtschaftsgipfel 1992 in München berichtet.

Ich hatte die Polizei darauf hingewiesen, daß nach meiner Auffassung **allein** die Teilnahme an Störhandlungen beim Weltwirtschaftsgipfel oder an geringfügigen Widerstandshandlungen, Beleidigungen und ähnlichen Delikten im Zusammenhang mit der Festnahme der Betroffenen ohne sonstige einschlägige Vorerkenntnisse die Speicherung in einer Staatsschutzdatei oder die Vergabe des KAN-Merkers 6 (bundesweite Speicherung) nicht rechtfertigt.

Inzwischen sind keine Personen mehr allein wegen Vorkommnissen im Zusammenhang mit dem Weltwirtschaftsgipfel 1992 gespeichert.

5.3.5 Dateien zur Gefahrenabwehr und zur Verfolgung von Straftaten und Ordnungswidrigkeiten (GAST)

Gem. Art. 47 Polizeiaufgabengesetz (PAG) hat die Polizei für den erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, in einer Errichtungsanordnung, die der Zustimmung des Staatsministeriums des Innern bedarf, die zu speichernden Inhalte der Datei festzulegen. Das Staatsministerium des Innern kann hierzu Rahmenregelungen durch Verwaltungsvorschrift erlassen. Bei der Datei GAST handelt es sich um eine solche vom Staatsministerium des Innern erlassene Rahmenregelung im Sinne dieser Vorschrift, in der der zulässige Umfang der zu speichernden Daten festgelegt wurde. Innerhalb dieses vorgegebenen Rahmens können die Polizeipräsidien bei Bedarf anlaßbezogen Dateien einrichten. Die Dateien können sowohl der Gefahrenabwehr als auch der Verfolgung von Straftaten oder Ordnungswidrigkeiten (GAST) dienen. Zumeist handelt es sich um sog. deliktgruppenspezifische

sche Dateien, die der polizeilichen Aufgabenerfüllung in Bezug auf bestimmte Erscheinungsformen der Kriminalität dienen sollen. Diese werden mir regelmäßig zur Kenntnisnahme und datenschutzrechtlichen Prüfung von den Polizeipräsidiem zugesandt (vgl. [Nr. 5.4](#)). Im Rahmen meiner datenschutzrechtlichen Prüfungen von Polizeidienststellen habe ich die Speicherungen in mehreren dieser Dateien geprüft. Eine Auswahl meiner Prüfungsfeststellungen ist im folgenden dargestellt:

5.3.5.1 Arbeitsdatei "Lagebild" (LAGEB)

Die Datei dient einem Polizeipräsidium und seinen Direktionen zur Erstellung eines aktuellen Lagebildes mittels eines EDV-unterstützten Meldewesen, der Zusammenführung der aus den Neuigkeitsmeldungen der einzelnen Polizeidienststellen gewonnenen Informationen bei den Polizeidirektionen und bei dem Polizeipräsidium. Erfasst werden Delikte der Eigentumskriminalität, Straftaten gegen höchstpersönliche Rechtsgüter sowie sonstige Ereignisse, Fahndungsansätze/-hinweise und -ersuchen. Eine themenmäßige Aufarbeitung ist durch eine Schlagwortliste möglich, die 190 verschiedene Begriffe enthält.

Bei einer Polizeidirektion habe ich Datenspeicherungen zu verschiedenen ausgewählten Schlagworten überprüft. Kritik habe ich insbesondere an den Speicherungen mit dem Schlagwort "Landfahrbewegung - LAND" geübt. Die Speicherungen betreffen polizeiliche Erkenntnisse über den Aufenthalt von Landfahrern unterschiedlicher Nationalität auf öffentlichen Plätzen in verschiedenen Orten des Direktionsbereiches. In Einzelfällen ist der Name des verantwortlichen Sippenführers gespeichert. Ferner wurden in den meisten Fällen alle Kfz-Kennzeichen der festgestellten Zug- und Wohnwagen dokumentiert. Mit einer Ausnahme waren im Zusammenhang mit der Feststellung der Landfahrer keine Sicherheitsstörungen dokumentiert. Auf Nachfrage wurde seitens der Polizeidirektion erklärt, daß die Speicherung von Landfahrbewegungen im Rahmen der vorbeugenden Bekämpfung von Straftaten insbesondere auf dem Einbruchssektor erforderlich sei. Dadurch sollen die Dienststellen aktuell über den Aufenthalt von Landfahrersippen im Zuständigkeitsbereich informiert werden. Dies diene zum einen der Unterstützung der Fahndung aber auch zum anderen als begleitende Maßnahme bei der Ermittlung von Straftaten, die nach dem Aufenthalt dieser Personengruppen bekannt werden.

Aus datenschutzrechtlicher Sicht habe ich gegen eine solche generelle personenbezogene Erfassung von Landfahrern bzw. ihrer Fahrzeuge große Bedenken. Auf meine erneute Nachfrage wurde mir das Beispiel eines Einbruchdiebstahl genannt, bei welchem drei tatverdächtige Landfahrer festgenommen und das Diebesgut sichergestellt wurde. Der - wenn auch nur beispielhaft - aufgeführte Vorgang rechtfertigt keinesfalls die pauschale Speicherung einer ganzen Gruppe zur vorbeugenden Verbrechensbekämpfung und damit ihre polizeiliche Einschätzung als potentielle Rechtsbrecher. Die generelle Speicherung von Landfahrern (Aufenthalt, Name des verantwortlichen Sippenführers, Kfz-Kennzeichen) halte ich für unzulässig, da sie eine ungerechtfertigte Diskriminierung einer ganzen Bevölkerungsgruppe darstellt. Ich habe gegenüber der betreffenden Polizeidirektion eine förmliche Beanstandung angekündigt und das Staatsministerium des Innern hiervon in Kenntnis gesetzt. In Ihrer Stellungnahme teilte dazu mir die Polizei lediglich mit, daß das Schlagwort "LAND" nunmehr in "ILAN" (offenbar: Informationen über Landfahrer) geändert wurde und daß Angehörige der Volksgruppe Sinti und Roma ähnlich wie Drückerkolonnen aufgrund ihrer Beweglichkeit zu den polizeilich relevanten Gruppen gehören, hinsichtlich derer die polizeiliche Erfahrung bestehe, daß von ihnen Gefahren für die öffentliche Sicherheit ausgehen können. Eine Speicherung sei nach der Rahmenerrichtungsanordnung GAST(vgl. [Nr. 5.3.5](#)) zulässig.

Dies trifft jedenfalls nicht zu. Rein abstrakte Gefahrenverursacher werden von dem Personenkreis der der Rahmenerrichtungsanordnung GAST nicht erfaßt. Ich habe das Staatsministerium des Innern deshalb aufgefordert, die pauschale und damit diskriminierende Speicherung von Sinti- und Roma-Gruppen zu unterbinden.

Das Ministerium hat eine Prüfung zugesagt und die Verwendung des Schlagwortes "ILAN" zunächst mit sofortiger Wirkung gesperrt. Bis zum Abschluß der Prüfung sei die Erhebung personenbezogener Daten in diesem Zusammenhang nur bei konkret eingetretenen Sicherheitsstörungen (z.B. Verfolgung von Ordnungswidrigkeiten und Straftaten) zulässig.

Vom Innenministerium erwarte ich eine zeitnahe Mitteilung des Prüfungsergebnisses. Die Beibehaltung der ursprünglichen Verfahrensweise halte ich - wie oben ausgeführt - nicht für zulässig.

5.3.5.2 Datei "Sittlichkeitsdelikte" (SITTE)

Die GAST-Datei SITTE wird bei einer Polizeidirektion geführt. Nach der zur Datei ergangenen Errichtungsanordnung dient sie der Bekämpfung von Sittlichkeitsdelikten im Bereich der Polizeidirektion, insbesondere der Zuordnung von Tätern zu bislang ungeklärten Straftaten anhand des modus operandi, der Täterbeschreibung sowie der Auswahl des Opfers durch den Täter. Neben Taten und Tätern von Vergewaltigung, sexuellen Mißbrauch von Kindern, sexueller Nötigung und Exhibitionismus werden unter der Kategorie "Sonstiges" auch "Delikte" erfaßt, die oben genannte Bereichen nicht zuzuordnen sind. Bei meiner datenschutzrechtlichen Prüfung der Polizeidirektion habe ich insbesondere diese Speicherungen auf ihre Zulässigkeit hin überprüft. Dabei stellte ich aber auch eine Speicherung zu einer männlichen Person fest, die allein deshalb in der Datei erfaßt worden war, weil sie bei einer polizeilichen Verkehrskontrolle mit Frauenkleidern in ihrem Pkw angetroffen wurde. Nachdem weder Anhaltspunkte für die Begehung von Straftaten zu der Person vorlagen, noch ein Gefährdungspotential aus dieser Neigung erkennbar war, war ihre Speicherung alleine aufgrund ihrer offenkundigen straflosen sexuellen Neigung unzulässig. Die Polizeidirektion hat mir mitgeteilt, daß die Mitarbeiter unterrichtet wurden. Das zuständige Polizeipräsidium und das Staatsministerium des Innern wurden von mir über den Sachverhalt in Kenntnis gesetzt.

5.3.6 INPOL-Fahndungsbildschirm

Im Informationssystem der Polizei (INPOL) erfolgen bundesweit Speicherungen, wenn die Personen z.B. zur Festnahme oder Aufenthaltsermittlung von der Justiz gesucht werden. Durch Bürgereingaben wurde mir bekannt, daß erhebliche Probleme auftreten können, wenn ein gesuchter Straftäter mit einer anderen Person identische Personalien hat oder der Gesuchte die Personalien einer anderen realen Person verwendet. Wenn nun der rechtmäßige Träger der Personalien in eine polizeiliche Kontrolle gerät, kann es zu einschneidenden Maßnahmen der Polizei gegenüber der nicht gesuchten Person kommen.

Grundsätzlich hat die Polizei für diese Fälle Vorsorge getroffen. In den meisten Fällen erhält die

nichtgesuchte betroffene Person, also der rechtmäßige Namensträger, eine schriftliche Bestätigung einer Polizeidienststelle, die ihn zusätzlich als rechtmäßigen Namensträger ausweist.

Diese Vorsorgemaßnahmen habe ich für ungenügend gehalten, weil es trotz dieses Hinweises gelegentlich zu einer Fehlinterpretation der einschreitenden Polizeibeamten kam und das Mißverständnis erst nach Stunden aufgeklärt werden konnte. Zur Vermeidung solcher Mißverständnisse der einschreitenden Polizeibeamten, habe ich gegenüber dem Staatsministerium des Innern verschiedene Vorschläge für die Formulierung eines Vermerks auf dem Fahndungsbildschirm gemacht, die zunächst nicht akzeptiert wurden. Nach weiterem Schriftwechsel hat sich das Staatsministerium des Innern bereit erklärt, zusätzliche und klarstellendere Formulierungen zu verwenden, die auch meines Erachtens künftig zur Minimierung von Fehlinterpretationen beitragen können.

Auf dem INPOL-Fahndungsbildschirm wird auf die Existenz eines rechtmäßigen und nicht gesuchten Namensträgers hingewiesen.

5.4 Überprüfung von Errichtungsanordnungen für Dateien

Gem. Art. 47 Polizeiaufgabengesetz (PAG) bedarf es für den erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, einer Errichtungsanordnung, für die die Zustimmung des Staatsministerium des Innern notwendig ist. Diese ist dem Landesbeauftragten für den Datenschutz mitzuteilen. Auch in diesem Berichtszeitraum sind wieder zahlreiche Errichtungsanordnungen für polizeiliche Dateien bei mir eingegangen. Sie werden von mir in datenschutzrechtlicher Hinsicht geprüft. In vielen Fällen hat meine Überprüfung ergeben, daß datenschutzrechtliche Verbesserungen nötig waren. Aufgrund meiner Forderungen und Anregungen wurden zahlreiche Errichtungsanordnungen von der speichernden Stelle geändert oder ergänzt. Insbesondere wurden folgende datenschutzrechtliche Verbesserungen vorgenommen:

- Verkürzung von Speicherungsfristen

- Schaffung differenzierter Speicherungsfristen für die unterschiedlichen Personenkategorien (z.B. Beschuldigter, Zeuge)
- Verzicht auf die Speicherung von Daten, die für den Dateienzweck nicht erforderlich sind
- Schaffung von Dokumentationspflichten für die Nachprüfbarkeit der Speicherungen (z.B. Darstellung der Grundlagen für die Annahme der Polizei eine Person gehöre zu einer bestimmten belasteten Personengruppe)

Forderungen zu einzelnen Errichtungsanordnungen sind nachfolgend dargestellt:

5.4.1 Errichtungsanordnung zur Datei "System zur Verknüpfung von Gewaltverbrechen" (VICLAS)

Das Staatsministerium des Innern hat mir die Errichtungsanordnung zur Datei "VICLAS" zugesandt. In einem zunächst bei einem Polizeipräsidium pilotierten und zwischenzeitlich bei der gesamten bayerischen Polizei eingesetzten Projekt sollen moderne Methoden zur Bekämpfung von Tötungsdelikten sowie Sexualdelikten unter Anwendung von Gewalt angewandt werden. Der Grundgedanke dieses neuen Verfahrens, welches in den USA und in Kanada seinen Ursprung hat, basiert insbesondere auf einer ausführlichen deliktsspezifischen Tatortanalyse und ggf. in geeigneten Fällen auf der Erstellung eines Täterprofils. Das Datenbanksystem VICLAS ergänzt diese beiden Instrumentarien, indem es ermöglicht, Serienzusammenhänge im Bereich der Tötungs- und Sexualdelikte auf überregionaler Ebene zu erkennen. Besonders vor dem Hintergrund der in der jüngsten Vergangenheit bekanntgewordenen Mord- und Mißbrauchsfälle, bei welchen insbesondere Kinder die Opfer waren, sehe ich die Notwendigkeit, Grundlagen für eine innovative Bekämpfung dieser Straftaten zu schaffen. Klarstellungsbedarf habe ich jedoch bei nachfolgendem Punkt gesehen und mich deshalb an das Staatsministerium des Innern gewandt:

Die Errichtungsanordnung sieht vor, daß "verdächtiges" Ansprechen von Kindern und Jugendlichen in der Datei VICLAS gespeichert werden soll. Ich habe das Staatsministerium des Innern gefragt, was darunter zu verstehen sei und wie die Grenzen zwischen Ansprechen und "verdächtigem Ansprechen" gezogen werden können. Das Ministerium hat mir dazu mitgeteilt, daß ein

"verdächtiges" Ansprechen dann vorliege, wenn das Verhalten einer Person ein sexuelles tatrelevantes Motiv erkennen lasse. Ob diese Voraussetzung zutrifft und ob deshalb eine Speicherung dieses Sachverhalts in Betracht kommt, werde nach Prüfung des Sachverhalts durch die fachlich zuständige Kriminaldienststelle und anschließend durch die eigens für dieses Projekt ins Leben gerufene Analysegruppe entschieden. Auch sei der Zugriff auf die Datei auf die Analysegruppe der Kriminalpolizei beschränkt. Unter Berücksichtigung dieser Ausführungen halte ich die Speicherung vorgenannter Sachverhalte grundsätzlich für vertretbar. Gleichwohl habe ich der Polizei bereits angekündigt, Datenspeicherungen in VICLAS einer datenschutzrechtlichen Stichprobenprüfung zu unterziehen.

5.4.2 Errichtungsanordnung zur Arbeitsdatei "Rauschgift" (ADR neu)

Die Datei dient der repressiven und präventiven Bekämpfung der Betäubungsmittelkriminalität einschließlich der Beschaffungs- und Begleitdelinquenz in Bayern. Der zu speichernde betroffene Personenkreis war in der Errichtungsanordnung teilweise zu weit gefaßt bzw. zu wenig konkret und deshalb weit auslegbar bezeichnet.

So sollten z.B. Personen gespeichert werden dürfen, deren Kenntnis erforderlich ist,

- "zur polizeilichen Sachbearbeitung im Rahmen eines Falles der Betäubungsmittelkriminalität ohne Täterbezug oder"
- "im Rahmen eines Falles der Betäubungsmittelkriminalität mit Anfangsverdacht, die Ermittlungen aber keinen strafrechtlichen Tatbestand ergaben."

Das Staatsministerium des Innern hat aufgrund meiner Anfrage diese beiden Personenkategorien aus der Errichtungsanordnung ersatzlos gestrichen. Gegen die mir zuletzt vorgelegten Fassung der Errichtungsanordnung bestanden keine datenschutzrechtlichen Bedenken mehr. Eine Prüfung der Speicherungspraxis in der Datei ADR neu habe ich für den nächsten Berichtszeitraum vorgesehen.

5.4.3 Errichtungsanordnung zur Datei "Pkw-Aufbrüche/Einbruchdiebstähle"

Die Datei soll die Bearbeitung von Pkw-Aufbrüchen/Einbruchdiebstählen innerhalb des Bereichs einer Polizeidirektion unterstützen. Neben Beschuldigten und Verdächtigen können auch Geschädigte, Fahrzeughalter, Mitteleiler und Anzeigerstatter gespeichert werden. Hierzu habe ich gegenüber dem Polizeipräsidium bemängelt, daß auch für den Kreis unbelasteter Personen ebenso wie für Straftäter die Vergabe der Höchstspeicherungsfrist von 10 Jahren vorgesehen ist. Die lange Speicherdauer von unbelasteten Personen halte ich in datenschutzrechtlicher Hinsicht für nicht vertretbar. Die Speicherung dieser Daten für einen angemessenen Zeitraum zum Zwecke der Vorgangsverwaltung, z.B. analog der Datei PSV für 5 Jahre erscheint erforderlich und damit zulässig. Das Polizeipräsidium teilte mir mit, daß auch unbelastete Personen wegen des Sachzusammenhangs ebenso lange wie Straftäter gespeichert bleiben müssen, z.B. um die Zuordnung von gestohlenem Gut auch bei späterem Auffinden gewährleisten zu können. Ich habe das Polizeipräsidium darauf hingewiesen, daß die Zuordnung von gestohlenem Gut auch aufgrund des Akteninhalts möglich sei und ich für eine so lange Speicherung von Geschädigten etc. in der Datei keine Erforderlichkeit sehe. Auch das Staatsministerium des Innern, an das ich mich deswegen gewandt habe, vertrat die Auffassung, daß es für die Verkürzung der Speichungsfrist von Personen, die keine Täter oder Tatverdächtige sind, aus den vom Polizeipräsidium genannten Gründen keinen Anlaß sehe. Zudem sei der Deliktsbereich "Wohnungs- und Pkw-Einbrüche" erfahrungsgemäß durch einen nichtvernachlässigbaren Anteil vorgetäuschter Anzeigen belastet. Um diese oft schadensträchtigen Fälle erkennen zu können, könne auf die personenbezogene Speicherung von Mitteilern und Anzeigerstattern nicht verzichtet werden.

Mit dieser Argumentation hat das Innenministerium eingeräumt, daß alle Geschädigten, Mitteleiler und Anzeigerstatter von der Polizei als potentiell Verdächtige vorgetäuschter Straftaten angesehen werden. Diese Sichtweise halte ich nicht für vertretbar. Sie führt zu einer unzulässigen Speicherung auf Vorrat, da konkrete Verdachtsgründe gegen die in der Datei erfaßten Personen zum Zeitpunkt der Speicherung nicht bestehen. Sollte sich im Einzelfall ein konkreter Verdacht einer Straftat gegen einen Angehörigen dieses Personenkreises ergeben, kann dieser als Tatverdächtiger für einen längeren Zeitraum gespeichert werden. Meinen Vorschlag, die Aussonderungsfrist bei Geschädigten, Mitteilern und Anzeigerstattern in der Errichtungsanordnung auf maxi-

mal fünf Jahre festzulegen, hat das Staatsministerium des Innern bisher abgelehnt.

5.5 Kontrolle von Datenerhebungsmaßnahmen

5.5.1 Verdachts- und ereignisunabhängige Kontrollen

Bereits in meinem letzten Tätigkeitsbericht hatte ich unter [Nr. 5.13](#) über meine Forderung gegenüber dem Staatsministerium des Innern berichtet, im Zusammenhang mit der in Art. 13 Abs. 1 Nr. 5 PAG geschaffenen erweiterten Möglichkeit zur Durchführung verdachts- und ereignisunabhängiger polizeilicher Kontrollen begleitende Erhebungen und Auswertungen zur Beurteilung des Erfolges dieser Maßnahme durchzuführen. Für die Bewertung dieser zusätzlichen polizeilichen Eingriffsbefugnis ist eine Erfolgskontrolle, die insbesondere Zahl und Ort der getroffenen Maßnahmen sowie ihre Ergebnisse (Erfolge) beinhalten sollte, von erheblicher Bedeutung. Das Innenministerium hatte meine Anregung leider abgelehnt und dies mit einem unvertretbar hohen zusätzlichen Arbeitsaufwand sowie mit der Schwierigkeit begründet, Erfolge konkreten polizeilichen Maßnahmen zuzuordnen. Hiergegen hatte ich ausgeführt, daß es gerade bei verdachtsunabhängigen polizeilichen Kontrollen möglich sein sollte, die Zahl der durchgeführten polizeilichen Kontrollen (getrennt nach Bundesautobahnen, Europastraßen und anderen Straßen) der Zahl der Fälle gegenüberzustellen, bei denen Anhaltspunkte für grenzüberschreitende Kriminalität weitere polizeiliche Maßnahmen notwendig gemacht haben.

Inzwischen habe ich mich bemüht, mir durch schriftliche Anfragen beim Innenministerium und verschiedenen Polizeidienststellen sowie anhand mehrerer Informationsbesuche auch bei örtlichen Dienststellen einen Überblick über Zahl, Durchführung und Ergebnisse der verdachtsunabhängigen Kontrollen zu verschaffen. Dabei hat sich bestätigt, daß nach wie vor bei den Polizeidienststellen keine Übersicht über die durchgeführten verdachts- und ereignisunabhängigen Kontrollen und deren Erfolge besteht, so daß im Nachhinein weder die Anzahl der Kontrollmaßnahmen feststellbar, noch deren rechtliche Einordnung möglich ist. Offenbar werden nur herausragende Ereignisse an vorgesetzte Dienststellen gemeldet.

Bei meinen Informationsbemühungen habe ich mein Augenmerk im besonderen auf die prakti-

sche Durchführung der in Art. 13 Abs. 1 Nr. 5 PAG bestehenden Befugnis gerichtet, verdachtsunabhängige Kontrollen nicht nur auf Bundesautobahnen und Europastraßen, sondern auch auf "anderen Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr" durchzuführen. Bereits im Gesetzgebungsverfahren hatte ich mich erfolglos u.a. dafür eingesetzt, die diesbezüglich sehr weite Fassung des Gesetzestextes dadurch zu präzisieren, daß Kontrolleinsätze auf solchen "anderen Straßen" nur von der Dienststellenleitung befristet angeordnet werden dürfen, um eine Beschränkung auf das unbedingt notwendige Maß zu erreichen. Meine Feststellungen haben hierzu ergeben, daß der Begriff der "anderen Straße von erheblicher Bedeutung für den grenzüberschreitenden Verkehr" grundsätzlich nicht durch interne Richtlinien oder Anweisungen näher bestimmt wird und auch diesbezüglich eine Dokumentation der polizeilichen Kontrollen nicht erfolgt. Die Polizei vertritt die Auffassung, daß aufgrund der wandelbaren tatsächlichen Gegebenheiten, wie sie nach dem polizeilichen Lagebild zu erkennen sind (vgl. Nr. 13.7 Vollzugsbekanntmachung zu Art. 13 PAG), grundsätzlich auch durch den einzelnen Polizeibeamten vor Ort festgelegt werden könne, welche Straße zur Zeit als "andere Straße" im Sinne des Gesetzes gelte. Allerdings haben meine Feststellungen bei einer **Polizeidirektion ergeben, daß dort die für Kontrollen in Frage kommenden Straßen anhand aktueller Lagebilder auf Direktions- bzw. Inspektionsebene per Anordnung festgelegt werden. Ich meine, daß diese Regelung geeignet wäre, aufgrund der Weite des gesetzlichen Tatbestands bestehende Mißbrauchsgefahren zu verringern.**

Ich werde die Entwicklung bei der praktischen Anwendung dieser noch relativ neuen polizeirechtlichen Befugnisnorm weiter aufmerksam beobachten.

5.5.2 Einsatz technischer Mittel in Wohnungen zur Gefahrenabwehr (präventiver Lauschangriff)

Die Polizei kann und konnte schon vor der Einführung des großen Lauschangriffs zur Strafverfolgung unter bestimmten Voraussetzungen durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen personenbezogene Daten zum Zwecke der Gefahrenabwehr erheben. Die Maßnahme darf nur durch den Richter, bei Gefahr im Verzug auch durch die im Polizeiaufga-

bengesetz genannten Dienststellenleiter angeordnet werden.

Alle fünf Maßnahmen aus den Jahren 1996 und 1997 habe ich bei einer Polizeidienststelle in datenschutzrechtlicher Hinsicht überprüft, wobei sich die Kontrolle nicht auf die Datenerhebung erstreckte, die gerichtlich überprüft worden ist.

Ich habe festgestellt, daß die richterliche Anordnung für jede einzelne Maßnahme vorlag. Gefahr im Verzug war in keinem Fall angenommen worden. Eine Benachrichtigung der von der Maßnahme betroffenen Personen erfolgte in den geprüften Fällen nicht. Eine solche vom Gesetz grundsätzlich vorgesehene Benachrichtigung unterblieb nach Angaben der Polizei, weil entweder wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden war oder weil eine Benachrichtigung nach Auffassung der Polizeidienststelle noch nicht ohne Gefährdung der öffentlichen Sicherheit möglich war. Das Polizeiaufgabengesetz läßt u.a. in diesen Fällen eine Ausnahme von der Benachrichtigungspflicht zu. Die Überprüfung ergab, daß in einem Fall der Nichtunterrichtung durch die von der Maßnahme Betroffenen, die dem organisierten Verbrechen zugeordnet werden können, weiterhin eine Gefährdung der Ermittlungen im Bereich der Organisierten Kriminalität und für Menschenleben gegeben war. In allen anderen Fällen wurde infolge des Ergebnisses der zunächst zur Gefahrenabwehr durchgeführten Überwachungsmaßnahmen gegen die Betroffenen ein strafrechtliches Ermittlungsverfahren eingeleitet. Die Gründe für die Nichtunterrichtung waren zum Zeitpunkt meiner Prüfung gegeben.

Ich habe gefordert, die Tatsache und die Gründe einer Nichtunterrichtung des Betroffenen nachprüfbar zu dokumentieren und ein Wiedervorlageverfahren einzuführen um zu gewährleisten, daß bei Wegfall der Gründe für das Absehen von der Benachrichtigung diese unverzüglich nachgeholt werden kann. Die Polizeidienststelle hat mir die künftige Dokumentation und die wiederkehrende Prüfung des Vorliegens von Hinderungsgründen zugesagt. Darüber hinaus ist die Polizei nach entsprechender Aufforderung bereit, eine Niederschrift über die Vernichtung des anlässlich der Maßnahmen gewonnenen Ton- und Bildmaterials durchzuführen. Andere Dienststellen, bei denen solche Unterlagen vorhanden sind, werden künftig benachrichtigt, damit sie ihrerseits die Vernichtung vornehmen können.

5.5.3 Telefonüberwachungsmaßnahmen

Nach den §§ 100 a ff. der Strafprozeßordnung darf unter den dort genannten Voraussetzungen die Überwachung und Aufzeichnung des Fernmeldeverkehrs (Telefonüberwachung) angeordnet werden. Bei einem Polizeipräsidium habe ich eine Reihe von Telefonüberwachungsmaßnahmen in datenschutzrechtlicher Hinsicht überprüft. Geprüft habe ich insbesondere, ob die richterliche Anordnung für die Maßnahme vorhanden war bzw., soweit diese bei Gefahr im Verzug auf Anordnung der Staatsanwaltschaft erfolgte, ob die Maßnahme nach 3 Tagen richterlich bestätigt wurde. Desweiteren habe ich geprüft, ob die durch die Maßnahme erlangten Tonträger und Unterlagen, die zur Strafverfolgung nicht mehr erforderlich waren, unter Aufsicht der Staatsanwaltschaft vernichtet und über die Vernichtung Niederschriften gefertigt wurden.

Ich habe festgestellt, daß in allen geprüften Fällen eine richterliche Anordnung oder Bestätigung zur Durchführung von Telefonüberwachungsmaßnahmen vorgelegen hatte. Bei allen geprüften Vorgängen konnte ich anhand der vorhandenen Dokumentation die Anordnung und den Vollzug der Löschung der Tonträger feststellen. Nicht nachvollziehbar war, aufgrund durchweg fehlender Dokumentation, die etwaige Anfertigung von Abschriften oder Aufzeichnungen über Verbindungsdaten, deren Anzahl und Verbleib bzw. deren Vernichtung.

Das Polizeipräsidium habe ich aufgefordert auch insoweit eine ausreichende Dokumentation sicherzustellen. Diese sollte Art und Anzahl der durch die Maßnahme gewonnenen Unterlagen, deren Verbleib sowie Durchführung und der Zeitpunkt der Vernichtung erkennen lassen. Sollten keine Abschriften oder Aufzeichnungen angefertigt worden sein, sollte dies gleichfalls im Interesse der Nachvollziehbarkeit dokumentiert werden. Eine Mitteilung des Polizeipräsidiums über das Veranlaßte steht noch aus.

Nach der Strafprozeßordnung sind die durch die Telefonüberwachungsmaßnahmen erlangten Unterlagen unverzüglich zu vernichten, wenn sie zur Strafverfolgung nicht mehr erforderlich sind. Die Pflicht zur Vernichtung kann also auch schon während eines Strafverfahrens entstehen, wenn sich herausstellt, daß die Unterlagen für die Strafverfolgung nicht oder nicht mehr benötigt werden, sei es, daß keine relevanten Erkenntnisse gewonnen wurden oder beweishebendliche

Erkenntnisse inzwischen durch andere Beweismittel bestätigt wurden. In einem von mir geprüften Fall hatte die Polizei der Staatsanwaltschaft mitgeteilt, daß sich aufgrund der Telefonüberwachung keine Hinweise auf die Straftat ergeben hätten. Die Anordnung der Staatsanwaltschaft das Material zu vernichten, erfolgte erst über zwölf Monate nach dieser Mitteilung der Polizei. Den Gründen dieser späten Löschanordnung werde ich noch nachgehen.

5.5.4 Einsatz von verdeckten Ermittlern/nicht offen ermittelnden Polizeibeamten

Bereits in meinem letzten Tätigkeitsbericht ([Nr. 5.2.2](#)) war ich auf Schwierigkeiten und praktische Bedeutung der Unterscheidung zwischen verdecktem Ermittler und nicht offen ermittelndem Polizeibeamten eingegangen. Ich hatte im einzelnen dargelegt, daß diese nach der Rechtsprechung des Bundesgerichtshofs anhand einer Gesamtwürdigung aller Umstände des Einzelfalles vorzunehmen ist.

Nachdem das Innenministerium eine entsprechende Ergänzung der Richtlinien, insbesondere die Klarstellung, daß ein Scheinaufkäufer nicht stets als nicht offen ermittelnder Polizeibeamter zu qualifizieren sei, abgelehnt hat, habe ich zur Feststellung der derzeitigen polizeilichen Praxis eine Reihe solcher Einsätze überprüft. Dabei habe ich festgestellt, daß die Abgrenzung zwischen verdecktem Ermittler und nicht offen ermittelnden Polizeibeamten vertretbar erschien. Insofern war eine deutliche Verbesserung im Vergleich zu meinen früheren Feststellungen zu verzeichnen. Der nicht offen ermittelnde Polizeibeamte wurde immer dann eingesetzt, wenn aufgrund der bisherigen polizeilichen Erkenntnisse nur mit einer kurzzeitigen Kontaktaufnahme mit dem Täter und dem schnellen Eintritt des Erfolges (Festnahme, Sicherstellung) zu rechnen war. In den von mir geprüften Fällen traf die entsprechende polizeiliche Prognose weitgehend zu. Seitens der geprüften Polizeidienststelle wurde mir mitgeteilt, daß ein verdeckter Ermittler immer dann eingesetzt werde, wenn der Einsatz eines nicht offen ermittelnden Polizeibeamten bei der Abwägung im Vorfeld erfolglos erscheint oder wenn absehbar sei, daß sich der Einsatz über längere Zeit bzw. über mehrere Kontakte hinziehen werde. Dies könne auch bei Scheinkaufverhandlungen ohne kurzfristig zu erwartenden Erfolg der Fall sein.

Insofern konnte ich feststellen, daß sich die polizeiliche Praxis an meinen Forderungen orientiert. Die Prüfung von konkreten Einsätzen dieser Art habe ich auch für den nächsten Berichtszeitraum vorgesehen.

5.5.5 Durchführung der DNA-Analyse (genetischer Fingerabdruck)

Am 22.03.1997 traten Bestimmungen in der Strafprozeßordnung in Kraft, welche die strafprozessualen Voraussetzungen für die Durchführung molekulargenetischer Untersuchungen (auch DNA- oder Genomanalyse genannt) regeln (vgl. [Nr. 7.1.7](#)). DNA-Analysen werden in Bayern in der Regel durch Sachverständige des Bayerischen Landeskriminalamtes durchgeführt. Die dortige praktische Durchführung war Gegenstand eines Informationsbesuches und später auch einer Prüfung.

Die Prüfung ergab im wesentlichen folgendes:

- Anonymisierung

Nach Angaben des BLKA werden mit zunehmender Tendenz derzeit 80% der Untersuchungsanträge in anonymisierter Form von der beantragenden Stelle (z.B. Polizei, Staatsanwaltschaft, Gericht) dem BLKA zugesandt. Trifft der Antrag in nicht-anonymisierter Form ein, wird dies beim BLKA nachgeholt, bevor der beauftragte Sachverständige den Auftrag erhält. Der vom BLKA definierte Anonymisierungsumfang wurde durch die Spurenkommission der Deutschen Gesellschaft für Rechtsmedizin festgelegt. Danach wird dem beauftragten Sachverständigen der Vorname, der erste Buchstabe des Familiennamens sowie das Geburtsjahr des Betroffenen zur Kenntnis gebracht. Das BLKA argumentierte, daß die Verwendung des Vornamens eines Betroffenen insbesondere wegen der Verwechslungsgefahr bei der Dechiffrierung durch die beantragende Stelle sowie wegen der Möglichkeit der Bestimmung von Geschlecht, verwandtschaftlicher Verhältnisse oder ethnischer Zugehörigkeiten notwendig sei. Außerdem sei aus der Sicht des BLKA mit dem Begriff "Name" nur der vollständige Nachname gemeint. Bei anderen

gesetzlichen Bestimmungen werde nach Nach-, Geburts- oder Familienname und Vornamen unterschieden, in der Strafprozeßordnung werde der Vorname von der Mitteilung nicht ausdrücklich ausgeschlossen.

Nach § 81 f Strafprozeßordnung ist dem Sachverständigen das Untersuchungsmaterial ohne Mitteilung des Namens, der Anschrift und des Geburtstages und -monats des Betroffenen zu übergeben. Es ist zutreffend, wie das BLKA ausführt, daß andere gesetzliche Bestimmungen deutlich die verschiedenen Namensarten unterscheiden. Gerade deshalb hätte der Gesetzgeber nicht "des Namens", sondern ausdrücklich "des Familiennamens" formuliert, wäre nur dieser gemeint. Der Begriff "Name" beinhaltet in diesem Zusammenhang nach meiner Auffassung jeglichen Namen oder Namensbestandteil, der eine erleichterte Identifizierung, wenn auch nur im Einzelfall, ermöglicht. Auch der Vorname kann im Einzelfall und im Hinblick auf vorhandenes Zusatzwissen zur Identifizierung geeignet und ausreichend sein. Die Verwendung des Vornamens beeinträchtigt den Schutzzweck der Vorschrift. Die Angabe des Geschlechtes und ggf. soweit erforderlich verwandtschaftlicher Verhältnisse oder ethnischer Zugehörigkeit ist dagegen durch die gesetzliche Regelung nicht ausgeschlossen und kann deshalb von der beantragenden Stelle mitgeteilt werden.

Bei einer Einverständniserklärung des Betroffenen mit der molekulargenetischen Untersuchung hält das BLKA eine Anonymisierung der Daten nicht für erforderlich. Ich teile diese Auffassung nicht. Es trifft zwar zu, daß die Strafprozeßordnung hierfür keine Anforderungen aufstellt. Regelungsgegenstand ist insoweit allein die zwangsweise Entnahme von Körpermaterial und dessen molekulargenetische Untersuchung. Gleichwohl bin ich der Auffassung, daß derjenige, der sich freiwillig untersuchen läßt, datenschutzrechtlich nicht schlechter gestellt werden sollte wie derjenigen, bei dem die Untersuchung zwangsweise angeordnet wird. Die Einverständniserklärung des Betroffenen erstreckt sich auch nicht auf eine Nichtanonymisierung, sondern auf die Untersuchung selbst. Das BLKA hat sich in diesem Punkt meiner Auffassung angeschlossen und wird künftig auch diese Untersuchungen in anonymisierter Form durchführen.

Das BLKA ist weiter der Auffassung, daß diejenigen Fälle nicht anonymisiert werden müssen, über die von den Medien bereits unter voller Namensnennung berichtet wurde. Im Gegensatz dazu sehe ich gerade hier die Notwendigkeit, die Grundsätze der Unabhängigkeit und Unbefangenheit des beauftragten Sachverständigen zu wahren und dafür Sorge zu tragen, daß dem Sachverständigen eine anonyme neutrale Untersuchung ermöglicht wird. Das BLKA zeigte für meine Bedenken kein Verständnis und wird wohl in diesen Fällen weiterhin von einer Anonymisierung absehen. Ich werde mich deshalb mit dem Innenministerium in Verbindung setzen.

- Praktische Umsetzung der Anonymisierung

Bei meiner Prüfung einer Reihe von Unterlagen zu DNA-Analysen habe ich festgestellt, daß über die meines Erachtens ohnehin unzureichende Anonymisierung hinaus weitere Mängel vorhanden waren. Teilweise war das gesamte Geburtsdatum oder der Nachname nicht anonymisiert. In einigen Fällen waren die Namen trotz Überzeichnung mit schwarzem Fettstift ohne großen Aufwand lesbar. Es sollte daher bei der Anonymisierung besser darauf geachtet werden, daß die entsprechenden Daten nicht trotzdem lesbar bleiben.

Das BLKA erklärte mir hierzu, daß dies ein technisches Problem sei, d.h. eine Frage der Qualität des verwendeten Schwärzungsstiftes und daß durch andere Maßnahmen der bereits jetzt erforderlichen Aufwand zur Anonymisierung in unvertretbarem Maß ansteigen würde. Dieses Argument lasse ich keinesfalls gelten. Die Anschaffung und Verwendung deckender Stifte kann keinen unverhältnismäßigen finanziellen Aufwand zur Sicherstellung des Datenschutzes in diesem Bereich bedeuten.

- Vernichtung des Untersuchungsmaterials

Nach Mitteilung des BLKA erfolgt die Vernichtung des Untersuchungsmaterials (isolierte DNA) sofort, wenn das Vergleichsmaterial nicht zu Spur paßt. Bei positiver Identität ist derzeit eine Aufbewahrungsdauer von zwei Jahren vorgesehen. Die Frist sei deshalb festgelegt worden, weil derzeit keine Rückmeldungsmechanismen seitens der bean-

tragenden Dienststelle hinsichtlich des Ausgangs des Verfahrens existieren und sie sei angelehnt an die Regelungen für die Aufbewahrung von Blutproben zur Blutproben-Alkoholbestimmung, die sich in der Praxis bewährt haben. Künftig werde das BLKA den Ablauf der zwei Jahre als Aussonderungsprüffrist anwenden.

Nach § 81 a Strafprozeßordnung sind dem Beschuldigten entnommene Blutproben oder sonstige Körperzellen unverzüglich zu vernichten, sobald sie für das Strafverfahren nicht mehr erforderlich sind. Die Festlegung einer Aussonderungsprüfung nach zwei Jahren erscheint mir willkürlich. Diese Frist kann in manchen Fällen zu lang, in anderen Fällen zu kurz sein. Sie wird der gesetzlichen Forderung einer unverzüglichen Vernichtung nicht gerecht. Daher wäre es meines Erachtens notwendig, daß die untersuchende Stelle bei Abschluß des Strafverfahrens über den Ausgang informiert wird.

- Technisch-organisatorische Maßnahmen

Das BLKA teilte mir mit, daß es folgende nach § 81 f Strafprozeßordnung erforderliche technisch-organisatorische Maßnahme zur Verhinderung molekulargenetischer Untersuchungen und einer unbefugten Kenntnisnahme durch Dritte getroffen habe:

Verhinderung der unbefugten Kenntnisnahme Dritter durch ein abgeschlossenes Sicherheitssystem des BLKA insgesamt und insbesondere der befaßten Abteilung Kriminaltechnik, in dem die Untersuchungen vorgenommen und Untersuchungsmaterialien aufbewahrt werden. Desweiteren durch Anonymisierung von Spuren und Vergleichsmaterial, die eine namensgebundene Suche ausschließt.

Verhinderung unzulässiger molekulargenetischer Untersuchungen durch organisatorische Maßnahmen. z.B. werden dienstlich ausschließlich Reagenzien und Bedarfsartikel zur Anwendung im erlaubten Untersuchungsumfang beschafft. Nicht erlaubte Untersuchungen würden auffallen. Die beteiligten Sachverständigen und Hilfskräfte sind auf Dienstpflicht zur Einhaltung der gesetzlichen Vorschriften angewiesen. Dies wird vom Sachgebietsleiter regelmäßig überwacht. Außerdem sei es derzeit nicht möglich, mit molekular-

genetischen Techniken besondere persönlichkeitsrelevante Merkmale, wie Charaktereigenschaften o.ä. festzustellen.

Die getroffenen Maßnahmen erscheinen mir nach dem jetzigen Kenntnisstand ausreichend.

Meine Korrespondenz mit dem Bayerischen Landeskriminalamt ist noch nicht abgeschlossen.

5.5.6 Erkennungsdienstliche Behandlung

Im Zuge von Prüfungen bei Polizeipräsidien habe ich festgestellt, daß in mehreren Fällen Polaroideaufnahmen von Betroffenen angefertigt wurden, obwohl sie nicht Beschuldigte eines strafrechtlichen Ermittlungsverfahrens oder einer konkreten Straftat verdächtig waren.

Als Rechtsgrundlage erkennungsdienstlicher Maßnahmen zur vorbeugenden Verbrechensbekämpfung kommen grundsätzlich § 81 b 2. Alt. StPO und Art. 14 Abs. 1 Nr. 2 PAG in Betracht. Nach § 81 b StPO dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen sowie Messungen und ähnliche Maßnahmen an ihm vorgenommen werden, soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist. Nach Art. 14 Abs. 1 Nr. 2 PAG kann die Polizei erkennungsdienstliche Maßnahmen vornehmen, wenn dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, **weil der Betroffene verdächtig ist, eine Tat begangen zu haben, die mit Strafe bedroht ist und wegen der Art und Ausführung der Tat die Gefahr der Wiederholung besteht.**

In den festgestellten Fällen schied § 81 b 2. Alt. StPO als Rechtsgrundlage aus, weil die Betroffenen - wie gesagt - nicht Beschuldigte waren. Die zuständige Polizeidienststelle stützte die Maßnahmen auf Art. 14 Abs. 1 Nr. 2 PAG. Sie vertritt die Auffassung, daß Art. 14 PAG solche erkennungsdienstliche Maßnahmen regelt, die von der Polizei ausschließlich im präventiven Bereich angefertigt werden. Hier seien Fälle denkbar, bei denen auf Art. 14 Abs. 1 Nr. 2 PAG zu-

rückgegriffen werden könne, wenn der Betroffene zwar nicht Beschuldigter ist, er aber ohne konkreten Tatverdacht - z.B. wegen angenommener Zugehörigkeit zu einer delinquenten Gruppierung - als Täter einer mit Strafe bedrohten Handlung in Betracht kommen kann.

Der Polizei gegenüber habe ich zum Ausdruck gebracht, daß die Bildaufnahmen auch nicht zulässigerweise auf Art. 14 Abs. 1 Nr. 2 PAG gestützt werden konnten, weil diese Vorschrift zwar die erkennungsdienstliche Behandlung von Personen ermöglicht, die etwa wegen Strafunmündigkeit, Schuldunfähigkeit oder bereits erfolgter rechtskräftiger Verurteilung nicht Beschuldigte sein können, ansonsten aber **einen konkreten Tatverdacht** voraussetzt. Es ist deshalb unzulässig, Art. 14 Abs. 1 Nr. 2 PAG in dem Sinne zu verstehen, daß diese Vorschrift die erkennungsdienstliche Behandlung eines jeden Nichtbeschuldigten gestattet, der aufgrund von einzelnen Erkennungsmerkmalen (z.B. punkerartige Kleidung, Besuch einschlägiger Lokale) Gruppierungen zugerechnet wird, aus denen heraus Straftaten begangen wurden. Dies stünde mit dem klaren Wortlaut der Vorschrift im Widerspruch.

Wegen der hiernach fehlenden gesetzlichen Voraussetzungen für die erkennungsdienstlichen Maßnahmen in den festgestellten Fällen werde ich das Polizeipräsidium auffordern, diese Praxis zu ändern und ggf. eine Beanstandung prüfen.

5.5.7 Bildaufnahmen bei Versammlungen

In meinem 17. Tätigkeitsbericht ([Nr. 5.9.1](#)) habe ich ausführlich zu der Frage Stellung genommen, unter welchen Voraussetzungen die Polizei bei Versammlungen Bild- und Tonaufnahmen anfertigen darf. Ich habe darauf hingewiesen, daß aufgrund der gesetzlichen Regelung in § 12 a Versammlungsgesetz einzelne Versammlungsteilnehmer nur dann gezielt beobachtet werden dürfen, wenn man aufgrund ihres Verhaltens oder aufgrund sonstiger Erkenntnisse mit Störungen durch diese Teilnehmer rechnen muß und wenn eine solche Beobachtung unter Berücksichtigung des Grundrechts der Versammlungsfreiheit zur Abwehr der bevorstehenden Störung der öffentlichen Sicherheit und Ordnung erforderlich und verhältnismäßig ist.

Aufgrund einer Eingabe habe ich davon Kenntnis erlangt, daß bei einer Protestveranstaltung gegen Atomkraft, die sich aus ca. 15 Teilnehmern zusammensetzte, von der Polizei Videoaufnahmen gefertigt wurden. Das Staatsministerium des Innern teilte mir hierzu mit, daß die Videoaufzeichnungen weder zum Zweck der Verfolgung etwaiger Verstöße gegen versammlungsrechtliche Auflagen noch zur Abwehr einer konkreten Gefahrenlage erstellt worden seien. Es habe sich vielmehr um reine **Übersichtsaufnahmen** gehandelt. Zweck der Aufnahmen sei ausschließlich die taktische Nachbereitung des Einsatzes auch im Hinblick auf mögliche zukünftige gleichgelagerte Einsatzlagen gewesen.

Als Übersichtsaufnahmen sind nur die Bildaufnahmen zu qualifizieren, die dazu dienen, ein Gesamtgeschehen festzuhalten. Auf die einzelnen Personen, die dabei zwangsläufig mit abgebildet werden, darf es nicht ankommen. Trotz fehlender spezialgesetzlicher Befugnisnormen hielt der Rechtsausschuß des Deutschen Bundestages Übersichtsaufnahmen für zulässig, weil sie nicht mit dem Ziel der Identifizierung einzelner Versammlungsteilnehmer hergestellt würden und deren Rechte daher nicht tangierten (BT-Drs. 11/4359, S. 17). Ich habe dazu ausgeführt, daß Übersichtsaufnahmen nicht zur Umgehung der in § 12 a VersammlG festgelegten Einschränkungen führen dürfen. Bei einer Versammlung mit lediglich 15 Teilnehmern sehe ich eine erhebliche Gefahr, daß durch die Videoaufzeichnung primär nicht der Verlauf der Versammlung als solcher, sondern die Identität und das Verhalten des individuellen Teilnehmers festgehalten wird.

Da im vorliegenden Fall die Voraussetzungen für die Anfertigung von Individualaufnahmen nach § 12 a Versammlungsgesetz nicht vorlagen, war für die Beurteilung der Rechtmäßigkeit entscheidend, ob es sich bei den erstellten Filmaufnahmen tatsächlich um sogenannte Übersichtsaufnahmen handelte. Die betreffenden Filme konnten von mir nicht mehr eingesehen werden, weil sie bereits kurze Zeit nach der Protestveranstaltung von der Polizei vernichtet worden waren. Es war ebenfalls nicht mehr möglich, zum Zwecke der zutreffenden Einordnung der Filmaufnahmen die genauen Umstände ihrer Anfertigung zu rekonstruieren. Die entscheidende Frage, ob im vorliegenden Fall tatsächlich nur Übersichtsaufnahmen angefertigt wurden, mußte daher letztlich offenbleiben.

Aufgrund dieser Erfahrung meine ich, daß in diesem äußerst sensiblen Grenzbereich zwischen

möglichst unbeeinträchtigt Wahrnehmung des Grundrechts auf Demonstrationsfreiheit und notwendiger polizeilicher Aufgabenerfüllung im Interesse aller Beteiligter geeignete Vorkehrungen zur Gewährleistung einer effektiven datenschutzrechtlichen Kontrolle getroffen werden sollten, um eine spätere Überprüfung polizeilicher Bildaufzeichnungen bei Versammlungen zu ermöglichen. Nachdem das Staatsministerium des Innern dargelegt hat, daß eine Dokumentation der näheren Umstände der polizeilichen Anfertigung von Übersichtsaufnahmen nicht praktikabel sei, habe ich darum gebeten, in Zukunft bei Versammlungen angefertigte polizeiliche Bildaufnahmen zum Zwecke der datenschutzrechtlichen Kontrolle zunächst aufzubewahren und mich hiervon umgehend zu unterrichten.

5.6 Kontrolle von Datenübermittlungen

5.6.1 Erhebungen für Finanzbehörden

Im Rahmen der Prüfung eines Polizeipräsidiums und aufgrund von Eingaben habe ich festgestellt, daß Polizeidienststellen auf entsprechende Ersuchen verschiedener Bezirksfinanzdirektionen und Finanzämter den Aufenthaltsort der betroffenen Personen ermittelten und den anfragenden Finanzbehörden mitteilten.

Während die bloße **Übermittlung** bei der Polizei bereits vorhandener Daten zum Aufenthaltsort der Betroffenen bei Vorliegen schutzwürdiger Interessen zulässig war, fehlten in einer Reihe von Fällen die gesetzlichen Voraussetzungen für eine polizeiliche **Datenerhebung** nach dem Polizeiaufgabengesetz. Die Polizei darf zwar personenbezogene Daten auch zur Erfüllung der ihr durch andere Rechtsvorschriften übertragenen Aufgaben erheben. Darunter sind jedoch nur diejenigen spezialgesetzlichen Normen zu verstehen, die der Polizei im einzelnen **bestimmte** Aufgaben zuweisen. Die allgemeinen Vorschriften zur Amtshilfe, wie z.B. § 111 Abgabenordnung oder Art. 4 ff. Bayerisches Verwaltungsverfahrensgesetz, fallen **nicht** darunter. Aus den Amtshilfenvorschriften folgt auch **keine generelle Befugnis der Polizei, Daten für andere Behörden zu erheben**. Soweit die Polizei Amtshilfe leistet und dazu Rechtseingriffe notwendig sind (wie z.B. Datenerhebung), muß sie auf Befugnisse zurückgreifen, die ihr **nach dem Polizeiaufgabengesetz oder nach speziellen Rechtsvorschriften** zustehen.

In den von mir abschließend geprüften Fällen dienten die Aufenthaltsermittlungen allein der Amtshilfe für die ersuchenden Finanzbehörden. Ersichtlich erfolgte die polizeiliche Datenerhebung auch nicht zu dem Zweck der Durchführung von Bußgeld- oder Strafverfahren, so daß es an der erforderlichen Rechtsgrundlage für den mit der Datenerhebung verbundenen Rechtseingriff fehlte.

Das Staatsministerium des Innern hat mir mitgeteilt, daß die nachgeordneten Polizeibehörden im Rahmen von Dienstbesprechungen entsprechend informiert wurden.

5.6.2 Datenübermittlungen an die Presse/Presseerklärung

Ein Eingabensteller teilte mit, daß die örtliche Zeitung im Zusammenhang mit dem Brand in einem Wohnhaus u.a. berichtete, daß der Brand "aus Verzweiflung über die bevorstehende Trennung von ihrem Ehemann von einer 44jährigen Frau" gelegt worden sei.

Meine datenschutzrechtliche Prüfung hat ergeben, daß die örtlich zuständige Polizeidirektion eine Presseerklärung veröffentlicht hatte, in deren Rahmen bekanntgegeben wurde, daß der Brand in dem Wohnhaus aller Wahrscheinlichkeit nach von der 44jährigen Wohnungsinhaberin gelegt worden sei und daß das Motiv für die Tat die bevorstehende Trennung von ihrem Ehepartner gewesen sein dürfte.

Ich habe diese Presseerklärung zum Anlaß genommen, gegenüber der Polizei auf die grundsätzliche Problematik bei der Übermittlung personenbezogener Daten durch die Polizei an die Medien einzugehen. Ich habe darauf hingewiesen, daß die Polizei bei ihrer Entscheidung, welche Daten der Presse übermittelt werden, eine Güter- und Interessenabwägung durchführen muß. Dabei ist zu berücksichtigen, daß die öffentliche Berichterstattung bei einer Straftat unter Namensnennung, Abbildung oder Darstellung des Beschuldigten regelmäßig eine erhebliche Beeinträchtigung seines Persönlichkeitsrechts darstellt (das auch für Straftäter gilt), auch weil der Betroffene dadurch ganz erhebliche langfristige persönliche oder berufliche Nachteile erleiden kann. Außerdem ist dem Persönlichkeitsrecht von Opfern, Zeugen und Familienangehörigen angemessen

Rechnung zu tragen. Sensationsbedürfnisse können ein Informationsinteresse der Öffentlichkeit nicht begründen (vgl. auch Nr. 8.1 der Richtlinie für die publizistische Arbeit nach Empfehlungen des Deutschen Presserats).

Die Polizei hat auch darauf zu achten, daß nicht nur die vollständige Bekanntgabe des Namens des Betroffenen eine Identifizierung ermöglicht, sondern auch Hinweise auf personenbezogene Angaben wie Wohnort, Alter, Beruf oder Familienverhältnisse usw. Rückschlüsse auf die Person des Täters oder des Opfers zulassen können.

Ich habe die Polizei darauf hingewiesen, daß nach meiner Auffassung die Presseerklärung der Polizei zu den Hintergründen des Wohnungsbrandes den datenschutzrechtlichen Anforderungen bei der Übermittlung personenbezogener Daten an die Medien nicht in vollem Umfang gerecht wird. Ein plausibler Grund dafür, daß die bevorstehende Trennung des Ehepartners als mögliches Tatmotiv für die Brandlegung durch die Wohnungsinhaberin bekanntgegeben wurde, ist nicht ersichtlich. Zur Befriedigung eines legitimen öffentlichen Informationsinteresses war es nicht erforderlich, über die ehelichen Differenzen der Betroffenen, die aufgrund der sonstigen Angaben (Alter der Wohnungsinhaberin, Ort und Zeitpunkt des Brandes) für Nachbarn und Bekannte identifizierbar war, zu berichten.

Das zuständige Polizeipräsidium hat sich dieser Beurteilung angeschlossen und mein Schreiben zum Anlaß genommen, in der präsidiumsinternen Informationsschrift einen Artikel zu dieser Thematik für alle nachgeordneten Dienststellen zu veröffentlichen.

5.7 Abfragen polizeilicher Informationssysteme

Die Abfrage polizeilicher Informationssysteme (z.B. des Kriminalaktennachweises) durch Polizeibedienstete ist eine Form der Datennutzung. Die Polizei darf personenbezogene Daten von polizeilich verantwortlichen Personen mit dem Inhalt polizeilicher Daten abgleichen. Personenbezogene Daten anderer Personen kann die Polizei nur abgleichen, wenn Tatsachen die Annahme rechtfertigen, daß dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist.

Die Polizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen.

Einige polizeiliche Informationssysteme, wie z.B. der Kriminalaktennachweis (KAN), stehen einer Vielzahl von Polizeibeamten für dienstliche Abfragen zur Verfügung. Zur Erledigung polizeilicher Aufgaben, z.B. zur Festnahme von gesuchten Straftätern, dem Schutz von Polizeibeamten oder Dritten vor Gefahren für Leib oder Leben und der Aufklärung von Straftaten halte ich die hohe Anzahl der zur Abfrage Berechtigten grundsätzlich für begründet. Je größer der Kreis der Abfrageberechtigten, desto größer ist auch die potentielle Gefahr des Mißbrauchs.

Der ganz überwiegende Teil der wegen Abfragen von mir geprüften Eingaben betraf das soziale Umfeld von Polizeibediensteten. Eine unzweifelhaft mißbräuchliche Abfrage konnte ich nur in einem Fall feststellen. Gleichwohl sind solche Abfragen meines Erachtens datenschutzrechtlich nicht unproblematisch, weil die Grenze von der dienstlich veranlaßten zur mißbräuchlichen oder strafrechtlich relevanten Nutzung personenbezogener Daten nicht immer klar gezogen werden kann.

Im Hinblick darauf habe ich gefordert, daß dienstlich veranlaßte Abfragen im sozialem Umfeld bzw. in eigener Sache grundsätzlich nicht von dem Betroffenen, sondern - nach Unterrichtung des Vorgesetzten - von einem unbeteiligten Polizeibeamten durchgeführt werden sollten. Ein Polizeipräsidium hat in seiner eigenen Zuständigkeit bereits Regelungen dazu getroffen. Eine landesweite Regelung entsprechender Maßnahmen zur Verbesserung des Datenschutzes halte ich für erforderlich. Das Staatsministerium des Innern hat dazu noch keine Stellungnahme abgegeben.

Bereits in der Vergangenheit habe ich immer wieder Maßnahmen zur Verbesserung des Datenschutzes bei Abfragen polizeilicher Informationssysteme gefordert (vgl. [16. Tätigkeitsbericht Nr. 5.5.3](#), [17. Tätigkeitsbericht Nr. 5.5.6](#)). Die insbesondere von mir geforderte Zusatzprotokollierung des Zweckes der Abfrage und eines eventuellen Aktenzeichens des betreffenden Vorgangs bei Abfragen im Informationssystem der Bayer. Polizei wurde vom Staatsministerium des Innern unter Berufung auf unverhältnismäßigen Verwaltungsaufwand und unzumutbarer Mehrbelastung

der EDV-Anlagen abgelehnt. Nicht zuletzt auch infolge der Diskussion um den in der Öffentlichkeit bekannt gewordenen Fall einer unzulässigen Datenspeicherung und -nutzung (vgl. [Nr. 5.3.1](#)) hat der Staatsminister des Innern die Einrichtung eines Zufallsgenerators angeordnet, durch welchen stichprobenartig Abfragen im Kriminalaktennachweis ausgewählt und durch den Dienstvorgesetzten des abfragenden Polizeibeamten unverzüglich auf die Zulässigkeit des Abrufs überprüft werden. Dieses System wird zwischenzeitlich landesweit eingesetzt. Zur Minimierung der Gefahr mißbräuchlicher Benutzung eines Bildschirms durch einen Nichtberechtigten wurde ebenfalls neu eine Abschaltautomatik eingeführt, sobald der Bildschirm für kurze Zeit nicht benutzt wird. Beide Maßnahmen begrüße ich, weil damit auch aus meiner Sicht die Gefahr unberechtigter Abfragen nicht unerheblich vermindert wird.

5.8 Kontrolle der Auskunftserteilung über Speicherungen in Dateien

5.8.1 Voraussetzungen der Auskunftserteilung

Die allgemeine Prüfung bei einem Polizeipräsidium sowie eine Bürgereingabe haben ergeben, daß bei Anträgen auf Auskunftserteilung über die zu einer Person gespeicherten Daten präzisierende Angaben zu Art und Umfang der polizeilichen Datenspeicherungen verlangt wurden und zumindest in einem Fall dem Antrag nicht entsprochen wurde, weil die vom Antragsteller verlangten Angaben nicht erteilt wurden. Als Begründung für diese Verfahrensweise wurde angeführt, daß es bei der Polizei keinen zentralen Nachweis über alle im Zusammenhang mit polizeilichen Sachbehandlungen angefallenen und gespeicherten personenbezogenen Daten gebe.

Nach dem Polizeiaufgabengesetz sollen zwar in dem Antrag die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, und der Grund des Auskunftsverlangens näher bezeichnet werden. Ohne Hinweis des Betroffenen auf einen bestimmten Sachverhalt oder eine bestimmte polizeiliche personenbezogene Sammlung ist diesem aber grundsätzlich Auskunft über Speicherungen im Kriminalaktennachweis und der Datei PSV (vgl. [Nr. 5.3.2](#)) zu erteilen. Dies bedeutet, daß in diesem Rahmen auch dann Auskunft zu erteilen ist, wenn der Betroffene - meistens aus Unkenntnis - sein Auskunftsverlangen nicht präzisiert.

Das betreffende Polizeipräsidium hat mitgeteilt, daß Antragsteller in Zukunft unter Beachtung

dieser Rechtsauffassung Auskunft erhalten.

5.8.2 Umfang der Auskunftserteilung

Nur wenn der Antrag des Betroffenen auf Erteilung der Auskunft über die zu seiner Person gespeicherten Daten ohne Hinweis auf einen bestimmten Sachverhalt oder eine bestimmte polizeiliche personenbezogene Sammlung gestellt wird, darf sich die Polizei bei ihrer Auskunft auf Speicherungen im Kriminalaktennachweis und in der Datei polizeiliche Sachbearbeitung/Vorgangsverwaltung - Verbrechensbekämpfung (PSV) beschränken. Aufgrund einer Bürgereingabe habe ich festgestellt, daß dem Betroffenen von einer Polizeidirektion die Auskunft über die zu seiner Person gespeicherten Daten in Anzeigetagebüchern und Neuigkeitsbögen verweigert wurde, obwohl er auf konkrete Sachverhalte, die eine polizeiliche Datenspeicherung vermuten ließen, hingewiesen hatte. Die Polizeidirektion hatte gegenüber dem Petenten die Auskunftsverweigerung damit erklärt, daß personenbezogene Daten in Anzeigetagebüchern und in Neuigkeitsbögen, die nicht Bestandteil einer Kriminalakte sind, den datenschutzrechtlichen Bestimmungen des Bayerischen Datenschutzgesetzes und des Polizeiaufgabengesetzes und damit dem Recht auf Auskunft nicht unterliegen würden.

Diese Auffassung ist falsch. Nach dem Polizeiaufgabengesetz kommt es für das Vorliegen eines Auskunftsanspruchs nicht darauf an, ob die personenbezogenen Daten in vormals von der Polizei manuell geführten Anzeigetagebüchern oder Neuigkeitsbögen oder in elektronischen Dateien erfaßt worden sind. In beiden Fällen liegen Datenspeicherungen vor, die grundsätzlich uneingeschränkt dem Auskunftsrecht unterfallen. Eine Auskunftsverweigerung mit dem Hinweis, Anzeigetagebücher und Neuigkeitsbögen seien interne polizeiliche Aufzeichnungen ist nicht zulässig.

Die Polizeidirektion hat auf mein Betreiben dem Petenten schließlich doch die Auskunft im vorgeschriebenen Umfang erteilt.

5.8.3 Ablehnung der Auskunft/Teilauskunft

Dem Betroffenen polizeilicher Datenspeicherungen ist grundsätzlich Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Die Erteilung der Auskunft darf nur unter den im Gesetz genannten Voraussetzungen abgelehnt werden. Im Hinblick auf die Bedeutung der Auskunft für die Wahrnehmung weiterer Datenschutzrechte, wie Löschung und Sperrung, ist, wenn ein Versagungsgrund nur für einen Teil der gespeicherten personenbezogenen Daten vorliegt, die Auskunft im übrigen zu erteilen (sog. Teilauskunft). Wird dem Betroffenen die Auskunft ganz oder teilweise verweigert, ist er darauf hinzuweisen, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann. Tut der Betroffene dies, prüfe ich, ob ausreichende Gründe für die Verweigerung der Auskunft vorgelegen haben und ob die Speicherung der personenbezogenen Daten, über die der Betroffene keine Auskunft erhält, zulässig ist.

Eine Reihe von Bürgern hat sich im Berichtszeitraum an mich gewandt. In zwei Fällen wurde den Petenten durch eine Polizeidirektion eine Auskunft mit dem Hinweis erteilt, daß dort keine weiteren Datenspeicherungen zu ihrer Person bestehen würden. Bei meiner Überprüfung habe ich allerdings festgestellt, daß diese Auskunft unrichtig war. Es handelte sich vielmehr jeweils nur um eine Teilauskunft, die als solche aber nicht erkennbar war. Ein solches Verhalten der Polizei ist unzulässig. Sie darf nicht, auch wenn die Polizei berechtigt ist, die Auskunft im Einzelfall teilweise zu verweigern, dem Betroffenen unzutreffende Auskünfte erteilen und ihn damit in die Irre führen. Auch Geheimhaltungsgründe können ein solches Verhalten nicht rechtfertigen. Vielmehr ist dem Betroffenen die Tatsache, daß nur eine Teilauskunft erteilt wurde, zu offenbaren.

Ich habe das zuständige Polizeipräsidium aufgefordert, dem Petenten die ihm zustehende Auskunft zu erteilen und für weitere derartige Verstöße eine Beanstandung angekündigt.

5.8.4 Generelle Ablehnung der Auskunft bei Betäubungsmittelhandel

Nach dem Polizeiaufgabengesetz unterbleibt die Auskunft u.a., soweit eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei, zu besorgen ist. Mit Blick hierauf hat das Staatsministerium des Innern festgelegt, daß **ohne Einzel-fallprüfung in allen Fällen** des unbefugten Rauschgifthandels eine Auskunft unterbleibt.

Dieser Auffassung bin ich entgegengetreten. Die Möglichkeit für den Bürger, sich zu informieren, welche öffentliche Stelle was über ihn weiß, ist ein entscheidender Bestandteil des Grundrechts auf informationelle Selbstbestimmung. Ohne entsprechende Kenntnis hat der Bürger keine Möglichkeit, evtl. bestehende Ansprüche z.B. auf Berichtigung oder Löschung seiner Daten durchzusetzen. Die Verweigerung der Auskunftserteilung stellt damit einen erheblichen Eingriff in seine Rechte dar, der unter Beachtung des Verhältnismäßigkeitsgrundsatzes auf besondere Ausnahmen nach Beurteilung des Einzelfalls zu beschränken ist.

Die **generelle** Ablehnung der Auskunftserteilung verstößt daher gegen das Gesetz. Art und Umfang des unbefugten Rauschgifthandels sind so verschiedenartig, daß nicht in allen Fällen der Auskunftserteilung eine Gefährdung der polizeilichen Aufgabenerfüllung angenommen werden kann. Dies gilt in besonderem Maße, wenn der Betroffene bereits von den gegen ihn geführten Ermittlungen und dem Tatvorwurf Kenntnis hat.

Das Staatsministerium des Innern ist nicht bereit, diese Praxis zu ändern. Ich muß deshalb inso- weit eine Beanstandung prüfen.

5.9 Mitwirkung an Gesetzen und Richtlinien

5.9.1 Änderung des PAG (Anpassung an die Änderung des Art. 13 des Grundgesetzes)

Mit Wirkung zum 27. März 1998 wurde Art. 13 des Grundgesetzes geändert. Hierdurch wurde zum einen die Möglichkeit geschaffen, die akustische Wohnraumüberwachung (sogenannter großer Lauschangriff) für den Bereich der Strafverfolgung einzusetzen (vgl. hierzu [Nr. 7.1.5](#)), zum anderen die bereits in der alten Fassung des Art. 13 GG enthaltene Möglichkeit der Wohnraumüberwachung zu Zwecken der Gefahrenabwehr modifiziert.

Die Bayerische Staatsregierung hat einen Gesetzentwurf vorgelegt, der die Anpassung des Polizeiaufgabengesetzes (PAG) und des Bayerischen Verfassungsschutzgesetzes (BayVSG) an diese Novellierung des Grundgesetzes zum Inhalt hat. Hierzu habe ich gegenüber dem Staatsministerium des Innern ausführlich Stellung genommen.

Ich habe unter Bezugnahme auf die Diskussion der Ausgestaltung der strafprozessualen Vorschriften zum sogenannten großen Lauschangriff angeregt, unter Einschränkung der schon bisher nach dem PAG gegebenen Möglichkeiten zum Abhören von Wohnungen die Erhebung personenbezogener Daten mit technischen Mitteln aus einem mittels Amts- oder Berufsgeheimnis geschütztem Vertrauensverhältnis im Sinne der §§ 53, 53 a StPO in und aus Wohnungen nur zur Abwehr einer **gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person** zuzulassen. Bei einem Einsatz technischer Mittel in wie auch außerhalb von Wohnungen sollte m.E. außerdem nicht in das **Beichtgeheimnis** eingegriffen werden. Die Datenerhebung in oder aus **Wohnungen von Nichtstörern** sollte nur zulässig sein, wenn die Gefahrenabwehr auf andere Weise nicht oder nicht rechtzeitig möglich wäre und dabei überwiegende Rechte und Pflichten dieser Personen nicht verletzt werden. Meines Erachtens ergibt sich die Berechtigung einer solchen Begrenzung um so mehr, wenn man bedenkt, daß der präventive Einsatz technischer Mittel in Wohnungen nicht nur auf Abhörmaßnahmen beschränkt ist, sondern auch Bildaufzeichnungen mit einschließt. Entsprechende Begrenzungen zum Schutz des Vertrauensverhältnisses von Amts- und Berufsgeheimnisträgern sollten auch bzgl. der Befugnis des Landesamtes für Verfassungsschutz zum verdeckten Einsatz besonderer technischer Mittel zur Informationsgewinnung

im Schutzbereich des Art. 13 GG (Art. 6 Abs. 4 BayVSG) eingeführt werden.

Diese Vorschläge haben leider, aber nicht unerwartet, keine Berücksichtigung gefunden.

Ich habe gegenüber dem Innenministerium desweiteren angeregt, den Gesetzentwurf der Staatsregierung im wesentlichen in folgenden Punkten zu ändern:

- Befristung des verdeckten Einsatzes technischer Mittel in Wohnungen nach dem PAG und dem BayVSG auf **vier Wochen**
- Verweisung in Art. 6 des BayVSG auf § 7 Abs. 1 und 2 des G-10-Gesetzes, wonach die Maßnahmen unter Verantwortung eines Bediensteten vorzunehmen sind, der die Befähigung zum Richteramt hat, und die Maßnahmen unverzüglich zu beenden sind, wenn die Voraussetzungen der Anordnung nicht mehr vorliegen oder die Maßnahmen nicht mehr erforderlich sind.

Die Staatsregierung ist dem zum Teil nachgekommen, eine Befristung der Maßnahme ist jedoch nach dem geänderten Gesetzentwurf bis zu **drei Monaten** möglich. Das zwischenzeitlich vom Bayerischen Landtag beschlossene Gesetz ist zum 01.08.1998 in Kraft getreten.

5.9.2 Europol

Das Europäische Polizeiamt (Europol) wird in Kürze seine Tätigkeit auf der Grundlage des Europol-Übereinkommens aufnehmen. Diese Konvention ist inzwischen von allen EU-Staaten ratifiziert worden und am 01.10.1998 in Kraft getreten.

Eine Reihe von Durchführungs- und Ausführungsbestimmungen zur Konvention, von deren Inkrafttreten die Tätigkeitsaufnahme von Europol abhängt, sind bereits ratifiziert. Dies gilt z.B. für das Europol-Immunitätenprotokoll, das für Europol-Bedienstete u.a. Immunität vor strafrechtlicher Verfolgung vorsieht.

Bereits in meinem letzten Tätigkeitsbericht ([Nr. 5.16](#)) hatte ich über den ersten Entwurf der Durchführungsbestimmungen zu den sog. Arbeitsdateien zu Analysezwecken berichtet. Hierzu faßten die Datenschutzbeauftragten von Bund und Ländern auf ihrer 53. Konferenz am 17./18.04.1997 folgende EntschlieÙung:

"Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich Nichtverdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 unterstützt werden soll.

Das Europäische Parlament hat in seiner EntschlieÙung zur Achtung der Menschenrechte gefordert, 'alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von Europol auszuschließen.'

Die nunmehr in Kraft getretenen Durchführungsbestimmungen sind im Vergleich zu dem ersten Entwurf wesentlich präziser und datenschutzfreundlicher gefaÙt.

Eine wesentliche Voraussetzung für die Arbeitsaufnahme von Europol ist auch mit der Einsetzung der gemeinsamen Kontrollinstanz geschaffen worden. Sie überprüft, ob durch die Verarbeitung von Daten bei Europol die Rechte von Personen verletzt werden. Ihr BeschwerdeauschuÙ entscheidet verbindlich über Beschwerden der Betroffenen im Zusammenhang mit der Auskunftserteilung, der Überprüfung gespeicherter Daten sowie deren Berichtigung und Löschung. Die deutschen Datenschutzbeauftragten sind durch den Bundesbeauftragten für den Datenschutz und den Landesbeauftragten von Sachsen-Anhalt in der gemeinsamen Kontrollinstanz vertreten. Sie haben sich bei den Beratungen der Geschäftsordnung der gemeinsamen Kontrollinstanz dafür eingesetzt, daß ihre Mitglieder Unabhängigkeit genießen, ihr Amt unparteilich wahrnehmen, die Behandlung von Beschwerden in einem fairen und grundsätzlich öffentlichen Verfahren erfolgt und der Anspruch der Betroffenen auf rechtliches Gehör gewahrt wird. Bei ihrer Mitarbeit in der gemeinsamen Kontrollinstanz werden sie auf die Einhaltung dieser Grundsätze achten.

Die Arbeitsaufnahme von Europol hängt u.a. noch vom Konsens über die Geschäftsordnung dieser gemeinsamen Kontrollinstanz ab. Dann wird Europol im Unterschied zur bisherigen vorläufigen Phase selbst Daten über Personen in eigenen Informations- und Analysedateien speichern, auswerten und an andere Stellen weitergeben.

Aus datenschutzrechtlicher Sicht behält die Kritik an dem strukturellen Mangel des Europol-Abkommens, daß eine parlamentarische Kontrolle der Behörde Europol fehlt, weiterhin ihre Berechtigung. Nicht befriedigend geregelt sind ferner die Rechtsschutzmöglichkeiten für den Bürger, der nur eingeschränkten Zugang zu ordentlichen Gerichten hat und weitgehend auf das Verfahren vor dem Beschwerdeausschuß der gemeinsamen Kontrollinstanz angewiesen ist. Wenig verständlich ist schließlich die Regelung über die Immunität für Europol-Bedienstete, die spätestens dann zu überdenken sein wird, wenn Europol - wie für die Zukunft geplant - einmal die Befugnis erhält, selbständig strafrechtliche Ermittlungsverfahren zu führen.

5.10 Datenschutzrechtliche Kontrolle während eines laufenden Ermittlungsverfahrens

Im Zusammenhang mit einem Ermittlungsverfahren wegen des Vorwurfs der unzulässigen Datenübermittlung durch einen Polizeibeamten bat ich zur Durchführung meiner datenschutzrechtlichen Prüfung die zuständige Polizeidienststelle um Mitteilung der bislang vorliegenden Ergebnisse der strafrechtlichen Ermittlungen. Polizei und Staatsanwaltschaft wiesen zunächst darauf hin, daß das staatsanwaltschaftliche Ermittlungsverfahren noch nicht abgeschlossen sei. Erst nach weiteren Bemühungen erhielt ich die gewünschten Informationen.

Ich habe dies zum Anlaß genommen, gegenüber Staatsministerium des Innern, Staatsministerium der Justiz und Polizei klarzustellen, daß ich die Frage des Vorliegens datenschutzrechtlicher Verstöße unabhängig von strafrechtlichen Ermittlungsverfahren in gleicher Sache prüfen und dazu auch Einblick in die staatsanwaltschaftlichen Ermittlungsergebnisse nehmen kann:

Nach [Art. 30 Abs. 4 Satz 1 BayDSG](#) ist zwar die Kontrolle durch den Landesbeauftragten für den Datenschutz über die **Erhebung** personenbezogener Daten **durch Strafverfolgungsbehör-**

den bei der Verfolgung von Straftaten **erst nach Abschluß des Strafverfahrens** zulässig. Im übrigen ergibt sich aus dem Gesetz aber keine besondere Einschränkung der Kontrollkompetenz des Landesbeauftragten für den Datenschutz in Bezug auf ein noch nicht abgeschlossenes Strafverfahren. Meine Überprüfung, ob im konkreten Fall oder in anderen Fällen, in denen sich die Notwendigkeit einer datenschutzrechtlichen Überprüfung ergibt, ein Verstoß gegen Datenschutzbestimmungen stattgefunden hat, setzt den Abschluß des jeweiligen Strafverfahrens nicht voraus, da sie nicht die Rechtmäßigkeit der Datenerhebung im Strafverfahren durch Strafverfolgungsbehörden zum Gegenstand hat. Die datenschutzrechtliche Kontrolltätigkeit erfolgt in diesen Fällen vollkommen unabhängig von der Arbeit der Strafverfolgungsbehörden und auch ohne Bindung an gerichtliche Entscheidungen oder die Beurteilung durch die Staatsanwaltschaft. Ob es im Einzelfall zweckmäßig ist, vor Beendigung der datenschutzrechtlichen Prüfung und Beurteilung den Abschluß und Ausgang behördlicher oder gerichtlicher Verfahren abzuwarten, wird allein von mir beurteilt und entschieden.

Gemäß [Art. 32 Abs. 1 Satz 2 BayDSG](#) sind dem Landesbeauftragten für den Datenschutz alle zur Erfüllung seiner Aufgaben notwendigen Auskünfte zu geben und auf Anforderung alle Unterlagen über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Einsicht vorzulegen. Dies betrifft auch polizeiliche Ermittlungsunterlagen, Strafakten und Informationen aus diesen, soweit ihre Kenntnis zur Erfüllung meiner Aufgaben erforderlich ist.

Abschließend habe ich die Polizei darum gebeten, bei zukünftigen Anfragen die erforderlichen Auskünfte ohne Zeitverzögerung zu erteilen und der gesetzlichen Verpflichtung nach [Art. 32 Abs. 1 Satz 2 BayDSG](#) zu entsprechen.

5.11 Sonstige Bürgereingaben

Aufgrund von Presseveröffentlichungen im Zusammenhang mit einer unzulässigen Speicherung personenbezogener Daten im Kriminalaktennachweis der bayerischen Polizei und der mißbräuchlichen Verwendung personenbezogener Daten im Berichtszeitraum haben mit steigender Tendenz wieder zahlreiche Bürger Anhaltspunkte für datenschutzrechtliche Verstöße bei der

Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch die Polizei an mich herangetragen.

Schwerpunkt der Eingaben waren wiederum Vermutungen, daß Polizeibeamte personenbezogene Daten für private Zwecke oder in ihrem sozialen Umfeld mißbräuchlich nutzen (vgl. [Nr. 5.7](#)). Ein häufiger Anlaß für Eingaben war auch die oft intensive und wiederholte Überprüfung der betroffenen Bürger bei polizeilichen Kontrollen, die von diesen auf polizeiliche Datenspeicherungen zurückgeführt wurde. Eingaben kamen auch von Betroffenen, die z.B. nach Anträgen auf Erteilung einer Erlaubnis (z.B. Waffenerlaubnis) oder anlässlich seiner Bewerbung bei bestimmten öffentlichen oder sicherheitsgefährdeten Stellen von der Übermittlung polizeilicher personenbezogenen Daten erfahren hatten und wegen der Datenspeicherung und -übermittlung eine Ablehnung hinnehmen mußten. In solchen Fällen habe ich, soweit Anhaltspunkte auf Rechtsverletzungen vorlagen, die Zulässigkeit der polizeilichen Datenverarbeitung geprüft.

Meine datenschutzrechtliche Überprüfung dieser Sachverhalte hat ergeben, daß bei einem weit überwiegenden Teil der Beschwerdeführer keine Rechtsverletzungen vorgelegen hatten. In einigen Fällen habe ich Verstöße festgestellt. Zur Behebung dieser Mängel habe ich die betroffenen Polizeidienststellen im Einzelfall aufgefordert, Daten zu löschen, zu berichtigen, Speicherungsfristen zu verkürzen und polizeiliche Unterlagen zu vernichten. Bei gravierenden Verstößen habe ich eine förmliche Beanstandung ausgesprochen. Da die Verstöße meines Erachtens häufig auf die unzureichende Kenntnis datenschutzrechtlicher Bestimmungen zurückzuführen waren, habe ich stets besonderen Wert darauf gelegt, Maßnahmen zu fordern, welche geeignet sind, die Wissensdefizite bei Bediensteten der bayerischen Polizei zu minimieren, wie z.B. Regelungen, Dienstunterrichte, Besprechungen und dienstaufsichtliche Maßnahmen.

6. Verfassungsschutz

6.1 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Bereich des Verfassungsschutzes waren:

- Allgemeine Kontrolle von Dateien und Karteien
- Überprüfung von Errichtungsanordnungen für Dateien und von internen Arbeitsanweisungen
- Kontrolle von Datenübermittlungen
- Bürgereingaben

6.2 Ergebnis meiner Prüfungen und Bewertung von Grundsatzthemen

Während des Berichtszeitraums habe ich beim Landesamt für Verfassungsschutz wieder ein- und mehrtägige Prüfungen vorgenommen und mich wegen datenschutzrechtlicher Grundsatzthemen mit dem Landesamt für Verfassungsschutz auseinandergesetzt. Einen Teil meiner Feststellungen habe ich im nachfolgenden dargestellt:

Eine Vielzahl von Themen im Zusammenhang mit der nachrichtendienstlichen Tätigkeit des Landesamtes unterliegen naturgemäß dem Geheimschutz und können deshalb auch von mir nicht veröffentlicht werden. Bei meinen Prüfungen habe ich festgestellt, daß das Landesamt für Verfassungsschutz den Datenschutz im Rahmen seiner gesetzlichen Befugnisse nach dem Bayerischen Verfassungsschutzgesetz (BayVSG) grundsätzlich wahrt.

6.2.1 Speicherungen im Zusammenhang mit dem Münchner Weltwirtschaftsgipfel 1992

Im 17. Tätigkeitsbericht (vgl. [Nr. 6.4.5](#)) habe ich ausgeführt, daß ich bei einer Reihe von Speicherungen im Zusammenhang mit polizeilichen Festnahmen beim Münchner Weltwirtschaftsgipfel 1992 (MWG '92) die Erforderlichkeit zur Aufgabenerfüllung des Landesamtes für Verfas-

sungsschutz nicht feststellen konnte und es deshalb erneut um Stellungnahme gebeten habe.

Das Landesamt für Verfassungsschutz hat mir zwischenzeitlich mitgeteilt, daß die Datenspeicherungen zum MWG '92 nochmals überarbeitet wurden. Die zur Aufgabenerfüllung noch erforderlichen Informationen seien zusammengefaßt, das übrige Material vernichtet worden. Nach Auffassung des Landesamtes für Verfassungsschutz dient die Vorhaltung der verbliebenen Datenspeicherungen der notwendigen Dokumentation des Ablaufs des MWG '92, der im Vorfeld gegen diesen geplanten und durchgeführten Aktionen und der daran beteiligte Gruppierungen.

Die verbleibenden Datenspeicherungen habe ich deshalb auf ihre Erforderlichkeit für die Aufgabenerfüllung des Landesamtes überprüft.

Insbesondere hinsichtlich des Großteils der von der Polizei damals festgenommenen Personen habe ich keine Erforderlichkeit für eine listenmäßige Speicherung gesehen. Bis auf wenige Ausnahmen wurden deren Daten von der Polizei zwischenzeitlich gelöscht (vgl. [Nr. 5.3.4](#)), weil sich entweder kein Nachweis für eine Straftat oder extremistische Bestrebungen ergeben haben. Das Landesamt für Verfassungsschutz hat mir daraufhin mitgeteilt, daß die unbelasteten Personen im Zusammenhang mit dem MWG '92 nicht mehr gespeichert werden. Die Vorhaltung der jetzt damit noch vorhandenen Unterlagen zum MWG '92 sehe ich aus datenschutzrechtlicher Sicht für die Aufgabenerfüllung des Landesamtes, z.B. zur Vorbereitung und Planung von Einsätzen zu künftigen ähnlichen Veranstaltungen, als vertretbar an.

6.2.2 Beobachtung der Scientology-Organisation durch das Landesamt für Verfassungsschutz

Die Innenminister von Bund und Ländern haben anlässlich ihrer Konferenz am 05./06.06.1997 festgestellt, daß bei der "Scientology-Organisation" Anhaltspunkte für verfassungsfeindliche Bestrebungen vorliegen und deshalb der Beobachtungsauftrag durch die Verfassungsschutzbehörden eröffnet ist. Bereits im Vorfeld des offiziellen Beobachtungsauftrags habe ich mit dem Landesamt für Verfassungsschutz die datenschutzrechtlichen Grenzen von personenbezogenen

Speicherungen in diesem Bereich erörtert. Mein Anliegen ist es, daß nur Personen im Zusammenhang mit Scientology-Organisationen von Datenspeicherungen betroffen werden, zu denen ausreichende Anhaltspunkte für eine extremistische Betätigung vorliegen. Auf entsprechende Einschränkungen habe ich hingewirkt, die in Regelungen des Landesamtes ihren Niederschlag gefunden haben. Nachdem ich mich über die Arbeit des Landesamtes für Verfassungsschutz in diesem Bereich mehrfach informiert habe, werde ich im nächsten Berichtszeitraum eine Prüfung von Datenspeicherungen im Zusammenhang mit Scientology-Organisation beim Landesamt für Verfassungsschutz vornehmen.

6.2.3 Speicherungs- und Wiedervorlagefristen in den Dateien des Landesamtes für Verfassungsschutz

Bei meiner Prüfung von Speicherungen in Dateien des Landesamtes für Verfassungsschutz, insbesondere im Hinblick auf die Einhaltung der Speicherungs- und Wiedervorlagefristen habe ich festgestellt, daß in den meisten Fällen eine mit der Speicherdauer identische Wiedervorlagefrist vergeben wurde. Diese Speicherungspraxis halte ich für unzureichend. Denn nach Art. 8 Abs. 2 Satz 2 Bayerisches Verfassungsschutzgesetz (BayVSG) ist nach festgesetzten Fristen zu entscheiden, ob die Voraussetzungen der Löschung und Vernichtung von Daten oder Akten vorliegen. Nach Art. 9 BayVSG sind in der Errichtungsanordnung zu einer automatisierten Datei sowohl Überprüfungsfristen als auch die Speicherdauer festzulegen. Nach meiner Auffassung ergibt sich daraus die Erforderlichkeit der Festlegung der von Speicherungsfristen unabhängigen Wiedervorlagefristen. Auch die mir bekannten Verwaltungsvorschriften zur Datenspeicherung beim Verfassungsschutz unterscheiden meines Erachtens klar zwischen Speicherungsfristen einerseits und Überprüfungsfristen, also Wiedervorlagefristen, andererseits. Ein zeitliches Zusammenfallen von Überprüfungs- und Speicherungsfrist würde den Sinn und Zweck einer Wiedervorlagefrist leerlaufen lassen. Ich könnte die Arbeitsanweisung - im Gegensatz zu meinem Vorgänger - ohne eine solche gesonderte Festlegung nicht akzeptieren.

Das Landesamt für Verfassungsschutz hat sich meiner Auffassung angeschlossen und nun eine Arbeitsanweisung vorgelegt, die von der Speicherungsfrist unabhängige Wiedervorlagefristen

vorsieht.

6.2.4 Arbeitsanweisung für die Speicherung und Löschung personenbezogener Daten beim Landesamt für Verfassungsschutz

Das Landesamt für Verfassungsschutz hat mir eine grundlegend überarbeitete Fassung seiner Arbeitsanweisung für die Speicherung und Löschung personenbezogener Daten mit der Bitte um datenschutzrechtliche Bewertung übersandt.

Mein Hauptanliegen war es insbesondere, Personen von einer Speicherung durch das Landesamt auszunehmen oder die Speicherdauern zu verkürzen für die nach meiner Auffassung nur unzureichende oder nur ungesicherte Anhaltspunkte für eine z.B. extremistische Betätigung vorlagen. Entsprechende Forderungen habe ich an das Landesamt gerichtet. Das Landesamt hat meine Anregungen zum Teil aufgegriffen und durch Streichungen, Einschränkungen und Klärstellungen in seiner Arbeitsanweisung umgesetzt. Zu einzelnen Forderungen ist die Diskussion mit dem Landesamt noch nicht abgeschlossen. Aus Gründen des Geheimschutzes kann ich zu dem Inhalt der Arbeitsanweisung und zu meinen datenschutzrechtlichen Forderungen im einzelnen hier keine Aussagen treffen.

6.2.5 Einführung eines Textverarbeitungssystems beim Landesamt für Verfassungsschutz

Das Landesamt für Verfassungsschutz hat mich darauf hingewiesen, daß es die Einführung eines modernen Textverarbeitungs-, Tabellenkalkulations- und Grafikprogramms plane. Wegen der Vielfalt der Einsatzmöglichkeiten eines modernen Textverarbeitungssystems stellten sich eine Reihe datenschutzrechtlicher Fragen.

Das System sollte zwar primär der Erstellung von Texten, Tabellen und Grafiken dienen, wie es in nahezu jeder modernen Verwaltung bereits Standard ist. Jedoch eröffnet es dem Landesamt für Verfassungsschutz daneben auch Möglichkeiten der fachlichen Nutzung, insbesondere der Recherche zum Zwecke der Aufgabenerfüllung. Eine solche Recherche kann mit individuellen

Suchmerkmalen, d.h. auch mit personenbezogenen Daten wie Namen, Geburtsdaten, Wohnadressen etc. durchgeführt werden und ist grundsätzlich über den gesamten Bestand der im Textverarbeitungssystem gespeicherten Dokumente möglich. Als Ergebnis einer Recherche können listenmäßig alle Dokumente am Bildschirm aufgezeigt werden, in denen der eingegebene Suchbegriff enthalten ist. Weiter besteht die Möglichkeit, die einzelnen Dokumente aufzuzeigen, die Liste auszudrucken oder in eine weitere Textverarbeitung zu übernehmen.

Das Textverarbeitungssystem ist deshalb als automatisierte Datei anzusehen, für die grundsätzlich eine -- erforderlich ist. Das Landesamt für Verfassungsschutz hat mir deshalb eine Errichtungsanordnung für die Datei vorgelegt. Dabei ist es meinem Anliegen gefolgt, die gezielte systematische Speicherung von personenbezogenen Daten und deren Auswertung oder Zusammenführung für fachliche Zwecke zu untersagen und dies in der Errichtungsanordnung festzuschreiben. Desweiteren dürfen nach der Errichtungsanordnung personenbezogene Daten, die vom Landesamt für Verfassungsschutz nach dem Verfassungsschutzgesetz nicht gespeichert werden dürfen, jedoch z.B. bei der Darstellung eines Sachverhalts - im Fließtext, in Tabellen oder in Grafiken unvermeidbar genannt werden müssen - nicht im Dokumentennamen oder in der Datei-Info (Verwaltungsprogramm) enthalten sein. Es werde sichergestellt, daß Dokumente, die zwölf Monate nicht mehr bearbeitet wurden, systemseitig und automatisch gelöscht werden. Unter Zugrundelegung dieser Beschränkungen habe ich der Errichtungsanordnung zugestimmt. Im nächsten Berichtszeitraum werde ich eine datenschutzrechtliche Prüfung von Speicherungen in der Datei vornehmen.

6.2.6 Registraturwesen beim Landesamt für Verfassungsschutz

Mit dieser Problematik habe ich mich bereits im 17. Tätigkeitsbericht (vgl. [Nr. 6.4.4](#)) befaßt. Das beim Landesamt für Verfassungsschutz verwendete EDV-unterstützte Registratur- und Schriftgutverwaltungssystem (REGA) ist geeignet, personenbezogene Daten des Empfängers und des Einsenders von Schreiben sowie der im Betreff des Schreibens genannten Person zu speichern und zu recherchieren. Wie bei der Einführung des Textverarbeitungssystems habe ich gefordert, die fachliche Recherche in dieser Datei durch eine entsprechende Regelung zu beschränken.

Fachliche Recherchen sind nur dann zulässig, wenn die gesetzlichen Voraussetzungen für die Speicherung der davon betroffenen Person nach dem Bayerischen Verfassungsschutzgesetz vorliegen. Bei Einsendern und Empfängern von Schriftstücken ist dies häufig nicht der Fall. Der Meinungsaustausch mit dem Landesamt für Verfassungsschutz zu dieser Frage ist nunmehr abgeschlossen. Es hat mir eine Dienstvorschrift übermittelt, die ausdrücklich festlegt, daß REGA ein reines Registratursystem ist und fachliche Recherchen unzulässig sind. Die Fachabteilungen haben auf REGA keinen Zugriff. Die Abteilungsleiter und Sachgebietsleiter haben die Einhaltung der Dienstvorschrift in ihrem Zuständigkeitsbereich im Rahmen der Dienstaufsicht laufend zu überwachen. Diese Einschränkungen habe begrüßt.

6.2.7 Entscheidung des Bayerischen Verfassungsgerichtshofes vom 11.11.1997

In einer umfangreichen Entscheidung hat sich der Bayerische Verfassungsgerichtshof aufgrund einer Popularklage mit mehreren Vorschriften des Bayerischen Verfassungsschutzgesetzes und des Bayerischen Datenschutzgesetzes befaßt. Über das Verfahren habe ich bereits in meinem 17. Tätigkeitsbericht ([Nr. 6.1](#)) berichtet.

Besondere Beachtung verdienen zwei Bereiche: Der Auskunftsanspruch des Betroffenen und die Kontrollbefugnisse des Datenschutzbeauftragten.

6.2.7.1 Der Auskunftsanspruch nach dem Bayerischen Verfassungsschutzgesetz

Art. 11 Abs. 1 Satz 1 Bayerisches Verfassungsschutzgesetz legt fest, daß kein Anspruch auf Auskunft über die beim Landesamt für Verfassungsschutz in Dateien oder Akten gespeicherten Informationen besteht. Wenn eine Person ein besonderes Interesse an einer Auskunft über die zu ihrer Person gespeicherten Daten hat, entscheidet über ihr Auskunftsbegehren das Landesamt nach pflichtgemäßem Ermessen. Nach der Entscheidung verstoßen die entsprechenden Bestimmungen des Bayerischen Verfassungsschutzgesetzes nicht gegen Art. 100 und 101 der Bayerischen Verfassung. Der vollständige Ausschluß eines Anspruchs auf Informationserteilung sei durch das überwiegende öffentliche Interesse begründet. Wenn aber schon der vollständige Aus-

schluß des Auskunftsanspruches zulässig sei, so dürfe in bestimmten Fällen erst recht die Erteilung einer Auskunft von einer Ermessensentscheidung abhängig gemacht werden.

Dieses Ergebnis zeigt, welche Bedeutung einer effektiven Kontrolle der Datenverarbeitung durch unabhängige Instanzen wie z.B. den Landesbeauftragten für den Datenschutz zukommt, da der Betroffene, dem keine Auskunft erteilt wird, eine Überprüfung der zu seiner Person gespeicherten Daten nicht selbst vornehmen kann.

6.2.7.2 Kontrollbefugnis des Datenschutzbeauftragten in Akten aus verdeckten Erhebungen

Der Verfassungsgerichtshof hat die Vorschrift des [Art. 30 Abs. 1 Satz 2 BayDSG](#) für verfassungsgemäß erachtet. Diese lautet: "Werden personenbezogene Daten in Akten verarbeitet oder genutzt, kontrolliert der Landesbeauftragte für den Datenschutz die Erhebung, Verarbeitung oder Nutzung, wenn der Betroffene ihm hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist oder wenn dem Landesbeauftragten für den Datenschutz hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen."

Der Verfassungsgerichtshof verneint die Notwendigkeit einer anlaßunabhängigen Kontrolle im Bereich verdeckter Datenerhebungen durch den Datenschutzbeauftragten. Er begründet dies damit, daß Einblick (durch den Datenschutzbeauftragten) in die Ermittlungsarbeiten der Polizei deren Arbeit "erheblich erschweren und unmöglich machen" würde.

Dazu bemerke ich, daß im Bereich der Datenverarbeitung in Dateien ich auch im Landesamt für Verfassungsschutz wie in jeder anderen öffentlichen Stelle das volle Prüfungsrecht habe, und zwar dann auch in den zugrundeliegenden Akten. Niemand - auch das Landesamt selbst nicht - hat in dieser vollen Prüfungscompetenz bisher ein Sicherheitsrisiko gesehen.

Ich halte eine uneingeschränkte Prüfkompetenz in Bereichen, in denen mit verdeckten Datenerhebungen gearbeitet wird, aus Gründen einer effektiven Kontrolle für zwingend erforderlich.

Aus dem Rechtsstaatsprinzip und dem Grundsatz effektiven Rechtsschutzes folgt nach meiner Auffassung, daß der Bürger eine Möglichkeit haben muß, eine gesetzeswidrige Beeinträchtigung eines Grundrechts durch die Einschaltung unabhängiger Kontrollinstanzen abzuwehren. Dies gilt in ganz besonderem Maße für Bereiche, in denen der Betroffene sein Grundrecht auf informationelle Selbstbestimmung nicht selbst schützen kann, wie dies bei der verdeckten Datenerhebung der Fall ist, von denen der Betroffene regelmäßig keine Kenntnis hat und von denen er auf Nachfrage im Regelfall auch nichts erfährt. Ich halte daher eine unabhängige, externe Kontrolle für geboten, um einen effektiven Schutz der Grundrechte, insbesondere des Grundrechts auf informationelle Selbstbestimmung zu gewährleisten. Gerade dann, wenn der Betroffene aus überwiegenden Sicherheitsinteressen über wesentliche Datenerhebungen, die seinen persönlichen Lebensbereich betreffen, nicht in Kenntnis gesetzt werden muß, erfordert dieses Defizit an persönlicher Kontrollmöglichkeit einen effektiven Ausgleich. Dieser kann nach meiner Auffassung nur durch eine Kontrolle unabhängiger und nicht an Weisungen gebundene staatliche Organe erfolgen. Scheidet aber faktisch eine Kontrolle durch Gerichte aus, weil diese nicht angerufen werden, weil der Betroffene selbst nichts von dem Grundrechtseingriff weiß, so bleibt als unabhängige Kontrollinstanz nur der jeweils zuständige Landesbeauftragte für den Datenschutz. Dies ist insbesondere im Bereich des Verfassungsschutzes von Bedeutung, weil hier eine Benachrichtigung des Betroffenen über eine Datenerhebung und Datenverarbeitung nur bei Maßnahmen nach dem G-10-Gesetz und nur dann erfolgt, wenn die Beschränkung des Brief-, Post- und Fernmeldeverkehrs beendet ist und eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann.

Eine dem [Art. 30 Abs. 1 Satz 2 BayDSG](#) entsprechende Vorschrift findet sich lediglich noch in den Datenschutzgesetzen des Bundes und des Landes Baden-Württemberg. Alle 14 anderen Landesdatenschutzgesetze enthalten eine derartige Einschränkung nicht. Gleichwohl ist dort die vom Verfassungsgerichtshof befürchtete Beeinträchtigung der Arbeit der Verfassungsschutzbehörden durch die Kontrollbefugnis des Datenschutzbeauftragten nicht festgestellt worden.

7 Justiz

7.1 Gesetzgebungsverfahren

7.1.1 Justizmitteilungsgesetz

Nach jahrelangen Vorarbeiten ist das Justizmitteilungsgesetz (JuMiG) verabschiedet worden und am 01.06.1998 in Kraft getreten. Dieses Gesetz regelt im wesentlichen die Befugnisse von Gerichten und Staatsanwaltschaften, **von Amts wegen** personenbezogene Daten an öffentliche Stellen zu übermitteln.

Bereits in meinem 17. Tätigkeitsbericht ([Nr. 7.1.2](#)) habe ich meine Hauptkritikpunkte an den damaligen Entwürfen des Justizmitteilungsgesetzes dargelegt. Es waren dies die fehlende Anordnungscompetenz für den Richter, Staatsanwalt oder Rechtspfleger in Fällen, in denen die Datenübermittlung einer besonders sorgfältigen Abwägung oder juristischen Bewertung bedarf, sowie die fehlende Pflicht zur Benachrichtigung des Betroffenen.

Leider haben diese datenschutzrechtlichen Forderungen im Gesetz selbst keinen Niederschlag gefunden. Ich habe mich daher sofort nach Verkündung des Gesetzes an das Staatsministerium der Justiz gewandt und dargelegt, daß ich es für notwendig halte, in den o.g. Fällen die Entscheidung darüber, ob eine Mitteilung erfolgen soll, dem Richter, Staatsanwalt oder einem Beamten des gehobenen Justizdienstes durch Verwaltungsvorschrift zuzuweisen. Ich habe ferner angeregt, durch eine entsprechende Regelung in den Verwaltungsvorschriften sicherzustellen, daß der Betroffene zumindest davon erfährt, daß im Gesetz die Möglichkeit vorgesehen ist, **auf Antrag** Auskunft über die übermittelten Daten und den Empfänger zu bekommen.

Zu den Verwaltungsvorschriften, einmal der Anordnung über Mitteilungen in Strafsachen (MiStra), zum anderen der Anordnung über die Mitteilungen in Zivilsachen (MiZi), haben die Datenschutzbeauftragten des Bundes und der Länder jeweils eine abgestimmte Stellungnahme abgegeben.

Eine Vielzahl unserer Forderungen wurden berücksichtigt. So wurde insbesondere in vielen Be-

stimmungen ein **ausdrücklicher Richter- bzw. Staatsanwaltsvorbehalt** aufgenommen.

Leider wurden auch einige Forderungen in der Endfassung der MiStra nicht aufgegriffen, so z.B.:

- Die einzelfallbezogene Dokumentation von Gründen, die zur Anordnung einer Mitteilung geführt hat, die nicht zwingend vorgeschrieben war.
- Keine zeitgleiche Unterrichtung der Betroffenen mit der Übermittlung personenbezogener Daten.

Zur Begründung wurde im wesentlichen auf den Aufwand für die Praxis hingewiesen.

Für die Mitteilungen in Zivilsachen enthielt bereits der Entwurf der Landesjustizverwaltungen eine Vielzahl von Entscheidungsvorbehalten für den Richter. Darüber hinaus wurde in einzelnen Fällen angeordnet, daß zugleich mit der Mitteilung der Betroffene über Inhalt und Empfänger der Mitteilung zu unterrichten ist und dadurch erst in die Lage versetzt wird, seine rechtlichen Interessen wahrnehmen zu können.

Da beabsichtigt ist, die MiZi und die MiStra jährlich an die Bedürfnisse der Praxis anzupassen, werde ich die Handhabung dieser Vorschriften in künftige Prüfungen miteinbeziehen und soweit dies veranlaßt ist, mit Verbesserungsvorschlägen an das Staatsministerium der Justiz herantreten.

7.1.2 Gesetz zum Schutz von Zeugen bei Vernehmungen in Strafverfahren und zur Verbesserung des Opferschutzes; Zeugenschutzgesetz

Die Vernehmung als Zeuge in einer Hauptverhandlung stellt für das Opfer einer Straftat - insbesondere für Kinder und Jugendliche - eine starke Belastung dar. Andererseits ist die Wahrheitsfindung im Strafprozeß auf Zeugen angewiesen. Einen Ausgleich versuchte hier zunächst der Bundesrat mit dem **Entwurf eines Gesetzes zum Schutz kindlicher Zeugen**.

Nachfolgend haben die Fraktionen der CDU/CSU und der F.D.P. den **Entwurf eines Gesetzes zum Schutz von Zeugen bei Vernehmungen im Strafverfahren** (Zeugenschutzgesetz) vorgelegt.

Aufgrund dieser Entwürfe und der beginnenden öffentlichen Diskussion haben wir Datenschutzbeauftragten des Bundes und der Länder schon auf unserer 54. Konferenz in Bamberg am 23./24.10.1997 unter meinem Vorsitz eine **EntschlieÙung über die informationelle Selbstbestimmung bei Bild-Ton-Aufzeichnungen in Strafverfahren gefaÙt** ([Anlage 11](#)).

In der EntschlieÙung wurde deutlich gemacht, daÙ Wahrheitsfindung und Zeugenschutz im gerichtlichen Verfahren auch im Interesse des Datenschutzes liegen. Allerdings sind dabei wegen des besonderen Eingriffs von Videoaufzeichnungen in das Persönlichkeitsrecht Möglichkeiten und Grenzen des Einsatzes der Videotechnologie im StrafprozeÙ durch den Gesetzgeber festzulegen. Dabei sollten insbesondere folgende Forderungen berücksichtigt werden:

- Der Eindruck des Aussagegeschehens darf nicht gezielt verfremdet oder verzerrt werden.
- Zeugnisverweigerungsrechte müssen gewahrt bleiben.
- Eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz darf nur in Ausnahmefällen erlaubt sein.
- Eine Verwertung von Bild-Ton-Aufzeichnungen im Rahmen eines anderen Strafverfahrens sollte nur zulässig sein, soweit sie auch für Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.
- Eine Verwertung in einem anderen gerichtlichen Verfahren darf nur unter engen Voraussetzungen zulässig sein.
- Die Aufzeichnungen sind grundsätzlich spätestens mit dem rechtskräftigen Abschluß des Verfahrens zu vernichten.

Der Bundestag hat am 30.04.1998 ein **Gesetz zum Schutz von Zeugen bei Vernehmungen im Strafverfahren und zur Verbesserung des Opferschutzes** (Zeugenschutzgesetz) verabschiedet. Dieses ist am 01.12.1998 in Kraft getreten.

Dieses Gesetz erlaubt die Aufzeichnung der Vernehmung eines Zeugen auf Bild-Ton-Träger. Aufzeichnungen sollen regelmäßig erfolgen, wenn zu besorgen ist, daß der Zeuge in der Hauptverhandlung nicht vernommen werden kann und die Aufzeichnung zur Erforschung der Wahrheit erforderlich ist, sowie bei Personen unter 16 Jahren, die durch die Straftat verletzt worden sind.

Erfreulicherweise enthält das Gesetz auch die Einschränkung, daß die Verwendung der Bild-Ton-Aufzeichnung nur für Zwecke der Strafverfolgung und nur insoweit zulässig ist, als dies zur Erforschung der Wahrheit erforderlich ist.

Aus datenschutzrechtlicher Sicht bedaure ich insbesondere, daß das Gesetz kein Verbot der Vielfältigung von Bild-Ton-Aufzeichnungen vorsieht. Ich teile insoweit die Auffassung der großen Strafrechtskommission des Deutschen Richterbundes, die sich in ihrem Gutachten zur Stellung des Kindes in Strafverfahren einstimmig dafür ausgesprochen hat, daß die Videoaufzeichnung unter keinen Umständen aus der Hand der Justiz in die Verfügungsmacht anderer Verfahrensbeteiligter oder justizfremder Personen gelangen darf. Den Ausschluß der Übermittlung der Videoaufzeichnung an Verfahrensbeteiligte außerhalb von Staatsanwaltschaft und Gericht halte ich im Interesse einer Einschränkung der Mißbrauchsmöglichkeit (kommerzielle Verwertung in den Medien, Versuche, das Opfer zu beeinflussen) für erforderlich.

Weiter bedaure ich, daß das Gesetz darauf verzichtet, die Einwilligung als Voraussetzung einer Bild-Ton-Aufzeichnung vorzusehen. Der Betroffene, zu dessen Schutz die gesetzlichen Vorschriften geschaffen wurden, wird regelmäßig selbst am besten beurteilen können, welche Form der Vernehmung (herkömmlich oder als Bild-Ton-Aufzeichnung) für ihn subjektiv die geringere Belastung darstellt.

7.1.3 Gesetzgebungsarbeiten zu einem Strafverfahrensänderungsgesetz

In meinem letzten Tätigkeitsbericht habe ich unter [Nr. 7.1.1](#) über den Stand der Gesetzgebungsarbeiten zu einem Strafverfahrensänderungsgesetz berichtet. Kurz nach Redaktionsschluß zum letzten Tätigkeitsbericht hat die letzte Bundesregierung den Entwurf eines Strafverfahrensänderungsgesetzes 1996 vorgelegt, der gegenüber dem Vorentwurf völlig überarbeitet wurde und insbesondere Regelungen zu folgenden Bereichen enthielt:

- **öffentliche Fahndung** nach Beschuldigten und Zeugen (auch durch Inanspruchnahme von Publikationsorganen)
- **längerfristige Observation**
- Erteilung von **Auskünften aus Akten** und die **Akteneinsicht** für Gerichte, Staatsanwaltschaften, Behörden, Privatpersonen (auch für wissenschaftliche Zwecke)
- Verwendung personenbezogener Daten, die für Zwecke der Strafverfolgung erhoben wurden, auch für präventivpolizeiliche Zwecke
- **Auskunftsanspruch** des Betroffenen

In meiner Stellungnahme zu dem Gesetzentwurf habe ich zunächst darauf hingewiesen, daß nach wie vor Regelungen über die Aufbewahrung, Aussonderung und Vernichtung der Strafakten fehlen. Ich habe daran erinnert, daß die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits auf ihrer 49. Konferenz am 09./10.03.1995 entsprechende Forderungen aufgestellt hat (s. [Anlage 1](#)). Danach sollte der Gesetzgeber die grundlegende Entscheidung über die Aufbewahrungsdauer selbst treffen.

Ferner habe ich eine Regelung vorgeschlagen, wonach auch außerhalb einer mündlichen Verhandlung ein Schweigegebot durch das Gericht verhängt werden kann. Im übrigen habe ich mich insbesondere zu folgenden Bereichen geäußert:

1. Öffentlichkeitsfahndung

Regelungen über die internationale Fahndung fehlen völlig. Insbesondere im Hinblick darauf, daß die bayerische Polizei bereits mit der weltweiten öffentlichen Fahndung im Internet begonnen hat, sollte dieser Bereich keinesfalls aus dem Gesetzgebungsverfahren ausgeklammert werden. Die weltweite Fahndung nach einem Beschuldigten in der Öffentlichkeit beeinträchtigt dessen Persönlichkeitsrecht in einer bisher nie dagewesenen Art und Weise und sollte deshalb strengen Voraussetzungen unterworfen werden.

2. Akteneinsicht

Ich habe kritisiert, daß der Entwurf keinerlei Aussagen vorsieht über die Behandlung von Aktenteilen, die besonders sensible Daten, wie z.B. psychiatrische Gutachten, enthalten. Darüber hinaus finden sich zwar Zweckbindungsregelungen hinsichtlich der durch Akteneinsicht gewonnenen Informationen, jedoch hat eine Nichtbeachtung keine strafrechtlichen Folgen. Ich habe ferner deutlich gemacht, daß nicht verfahrensbeteiligten Personen nur bei der Darlegung eines **rechtlichen** Interesses Akteneinsicht gewährt werden sollte. Nach meiner Auffassung geht es nicht an, daß bereits bloße wirtschaftliche Interessen zu einer umfassenden Kenntnisnahme einer Vielzahl personenbezogener Daten berechtigen.

Im weiteren Gesetzgebungsverfahren hat der Bundesrat gravierende datenschutzrechtliche Verschlechterungen des Entwurfs der Bundesregierung beschlossen.

Die 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dies zum Anlaß genommen, ihre grundsätzliche Haltung zum Entwurf eines Strafverfahrensänderungsgesetzes 1996 zu verdeutlichen (s. [Anlage 4](#)).

Sie hat die Bundesregierung und den Deutschen Bundestag aufgefordert, bei den anstehenden weiteren Beratungen des Gesetzentwurfs die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Der Gesetzentwurf der letzten Bundesregierung ist durch Ablauf der Legislaturperiode der Diskontinuität verfallen. Dies bedeutet, daß auch 15 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts in weiten Bereichen des Strafverfahrensrechts die notwendigen Regelungen für die Erhebung und Verarbeitung personenbezogener Daten noch immer fehlen.

Ich hoffe, daß in der neuen Legislaturperiode diese dringend notwendige rechtliche Regelung der Datenverarbeitung im Strafverfahren bald in Kraft tritt und dabei die datenschutzrechtlichen Kritikpunkte Berücksichtigung finden.

7.1.4 Viertes Gesetz zur Änderung des Strafvollzugsgesetzes

In meinem 17. Tätigkeitsbericht ([Nr. 7.1.3](#)) habe ich über den vorläufigen Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes und dessen Defizite berichtet. Auf der Grundlage dieses vorläufigen Referentenentwurfs hat die letzte Bundesregierung das Gesetzesvorhaben in den Bundestag eingebracht.

Gegenüber dem vorläufigen Referentenentwurf enthielt dieser Entwurf einige datenschutzrechtliche Verbesserungen. Folgende meiner Vorschläge haben Eingang in den Gesetzentwurf gefunden:

- Freistellung des Schriftverkehrs des Gefangenen mit den Datenschutzbeauftragten des Bundes und der Länder von der Briefkontrolle.
- Verzicht auf die Verpflichtung zur Verwendung von Paketmarken
- Verkürzte Aufbewahrungsfristen für Gefangenenpersonalakten

Darüber hinaus habe ich begrüßt, daß die Verpflichtung vorgesehen ist, den Partner eines Telefongesprächs mit dem Gefangenen vor dem Beginn des Gesprächs über eine beabsichtigte Überwachung zu informieren.

Einige meiner Forderungen blieben aber unberücksichtigt:

- Im Gesetz selbst, nicht nur in Verwaltungsvorschriften, sollte Inhalt, Gliederung und Gestaltung der Gefangenenpersonalakte geregelt werden. Dies gebietet die zentrale Bedeutung dieser Akte für den einzelnen Strafgefangenen.

- In die Schweigepflicht gegenüber der Vollzugsanstalt über den Anstaltsarzt hinaus sollten nicht nur - wie geschehen - die Berufspsychologen oder Sozialarbeiter der Anstalt, sondern auch die in § 203 Abs. 3 StGB genannten Hilfspersonen der betroffenen Personkreise einbezogen werden.
- Auch Aktenteile, die "besonders sensible Daten" enthalten, nicht nur Gesundheitsakten und Krankenblätter, sollten von der Gefangenenpersonalakte getrennt geführt werden.
- Diesen besonderen Schutz verdienen insbesondere Unterlagen über psychologische oder sozialtherapeutische Behandlungen sowie Erkenntnisse aus der Überprüfung von Besuchern oder der Briefkontrolle.
- Für die Aufbewahrung von personenbezogenen Unterlagen sollten absolute gesetzliche Höchstfristen vorgeschrieben werden, die für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter 15 Jahre und für Gefangenenbücher 25 Jahre nicht überschreiten sollten.

Wegen Vorschlägen des Bundesrats, die eine massive datenschutzrechtliche Verschlechterung des Gesetzesentwurfs bedeutet hätten, hat sich die diesjährige Konferenz der Datenschutzbeauftragten des Bundes und der Länder durch ihren Vorsitzenden, den Hessischen Datenschutzbeauftragten, an den Bundesjustizminister gewandt und gebeten, insbesondere folgende Punkte nicht zu berücksichtigen:

- Lichtbilder und die Beschreibung körperlicher Merkmale, die während des Vollzugs entstanden sind, von der Vernichtung nach der Entlassung auszuschließen. Dies würde der Sache nach zu einer unzulässigen Datenspeicherung auf Vorrat führen. Die Aufbewahrung solcher Unterlagen für eine spätere Fahndung aufgrund eines neuen Tatverdachts nach zwischenzeitlicher Entlassung des Gefangenen erfolgt nicht mehr zu Zwecken des Strafvollzuges, sondern "vorsorglich" im Hinblick auf mögliche spätere Strafverfahren. Dies ist nicht Aufgabe des Strafvollzugs.
- Umwandlung einer Offenbarungsbefugnis für Ärzte, Sozialarbeiter und ähnliche Berufsgruppen in eine Mitteilungspflicht

- Zu lange Aufbewahrungsfristen, wie sie bereits der Vorentwurf vorgesehen hatte.

Immerhin diesen datenschutzrechtlichen Anliegen wurde in weitem Umfang Rechnung getragen. Das Gesetz ist am 01.12.1998 in Kraft getreten.

7.1.5 Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität (sog. großer Lauschangriff)

Bereits in unserer 52. Konferenz hatten wir Datenschutzbeauftragten des Bundes und der Länder einen Forderungskatalog beschlossen, der für den Fall der Einführung der akustischen Wohnraumüberwachung der Sicherung der Privatsphäre Rechnung tragen sollte ([Anlage 3](#)). Die vorgelegten Gesetzentwürfe haben diese Forderungen nur zum Teil berücksichtigt. Ich habe mich daher an die Staatsminister der Justiz und des Innern gewandt und in Übereinstimmung mit den übrigen Datenschutzbeauftragten u.a. folgende Kritikpunkte vorgebracht:

- Der vorgesehene Straftatenkatalog ist zu weit. Es muß sich zumindest um schwerste Straftaten, die die Rechtsordnung nachhaltig gefährden, handeln. Die vorgesehenen Formulierungen etwa im Bereich Bandendiebstahl, gewerbsmäßige Hehlerei und im Bereich des Betäubungsmittelgesetzes gewährleisten nicht, daß die unter diese Tatbestände fallenden leichteren Fallvarianten, wie z.B. jugendtypische Delikte, wie der bandenmäßige Kaufhaus- oder Fahrraddiebstahl oder Haschischrunden im Freundeskreis nicht als Voratbestände für eine elektronische Wohnraumüberwachung in Frage kommen.
- Regelungen zum Schutz von Berufsgeheimnissen fehlten. Das Vertrauensverhältnis zwischen Anwalt und Mandant, zwischen Arzt und Patient, zwischen Psychologen und Hilfesuchendem wird unzumutbar belastet, wenn beide mit der Möglichkeit heimlichen Abhörens rechnen müssen.

Ferner habe ich gefordert, daß die Zulässigkeit des Abhörens von Wohnungen Nichtbeschuldigter weiter eingeschränkt werden muß. Die bloße Vermutung, daß sich der Beschuldigte in den Räumen des Dritten aufhält, kann dafür nicht ausreichen, vielmehr sollten hierfür konkrete Anhaltspunkte bestehen. Dementsprechend wurde in den Gesetzentwurf zur Verbesserung der Be-

kämpfung der organisierten Kriminalität aufgenommen, daß Wohnungen Nichtbeschuldigter erst dann abgehört werden dürfen, wenn auf Grund **bestimmter Tatsachen** anzunehmen ist, daß sich der Beschuldigte in ihr aufhält.

Am 16.01.1998 hat der Deutsche Bundestag in zweiter und dritter Lesung diesem Gesetzentwurf zugestimmt. In diesem Zusammenhang wurde auch Art. 13 des Grundgesetzes geändert und damit die Voraussetzung für die **akustische Wohnraumüberwachung** ("großer Lauschangriff") im Bereich der Strafverfolgung geschaffen.

Nicht zuletzt auch aufgrund der Appelle des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz wurde der Entwurf dahingehend ergänzt, daß eine akustische Wohnraumüberwachung dann unzulässig ist, wenn sie sich gegen einen **Berufsgeheimnisträger** im Sinne des § 53 StPO richtet. Bei zur **Zeugnisverweigerung** berechtigten Angehörigen sowie bei den Berufshelfern ist zwar ein Lauschangriff nicht schlechthin unzulässig. Die gewonnenen Erkenntnisse dürfen aber nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes des Täters steht.

Unsere Forderungen im Hinblick auf den zu weiten Straftatenkatalog hat der Gesetzgeber hingegen nicht aufgegriffen.

7.1.6 Entwurf eines Gesetzes zur Änderung des Bundeszentralregistergesetzes

In der vergangenen Legislaturperiode hat das Bundesministerium der Justiz einen Referententwurf eines Vierten Gesetzes zur Änderung des Bundeszentralregistergesetzes vorgelegt. Der Entwurf greift meine seit langem erhobene Forderung nach Änderung des § 11 BZRG auf. Speicherungen strafgerichtlicher oder staatsanwaltschaftlicher Verfügungen der Einstellung eines Verfahrens wegen erwiesener oder vermuteter **Schuldunfähigkeit**, die derzeit praktisch lebenslang (bis zum 90. Lebensjahr des Betroffenen) im Register eingetragen sind, sollen nunmehr eingeschränkt und in Anlehnung an das System der Tilgung von Verurteilungen nach bestimmten Fristen aus dem Register entfernt werden.

Ich habe aber gegenüber dem Staatsministerium der Justiz zum Ausdruck gebracht, daß ich ein Sachverständigengutachten für die Eintragungen wegen Schuldunfähigkeit sowie die Pflicht zur

Unterrichtung des Betroffenen über solche Eintragungen für notwendig halte.

Durch eine gesetzliche Verpflichtung zur Einholung eines Sachverständigengutachtens wird der Praxis nach meiner Einschätzung nicht mehr abverlangt, als sie bei sorgfältiger Sachbehandlung ohnehin tun müßte. Angesichts des schwerwiegenden Eingriffs in das Persönlichkeitsrecht durch eine Eintragung ins Bundeszentralregister erscheint der damit verbundene Aufwand auch gerechtfertigt.

Das Gesetzgebungsverfahren ist in dieser Legislaturperiode nicht mehr zum Abschluß gebracht worden.

7.1.7 Molekulargenetische Untersuchungen im Strafverfahren und Aktivitäten zur Errichtung einer zentralen DNA-Analyse-Datei

7.1.7.1 Überblick

Zunehmend wurde im Berichtszeitraum bei der Verfolgung von Straftaten sog. biologisches Material als Spurenmaterial, sei es am Tatort oder beim Opfer, durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen, seien es Verdächtige, Opfer oder unbeteiligte Dritte, oder die Identität mit anderem Spurenmaterial unbekannter Personen festzustellen.

Im Hinblick auf die besonderen Gefährdungen des Persönlichkeitsrechts ist eine normenklare gesetzliche Grundlage sowohl für die Erhebung dieser Daten als auch für deren Speicherung erforderlich. Zu unterscheiden sind dabei die

- DNA-Analyse in einem konkreten Strafverfahren
- DNA-Analyse zum Zwecke künftiger Strafverfolgung, und
- Speicherung solcher Analyseergebnisse zu Zwecken künftiger Strafverfolgung.

Es ist vom Gesetzgeber selbst über die Voraussetzungen solcher gravierender Eingriffe und die notwendigen rechtsstaatlichen Sicherungen zu entscheiden, wie z.B. über ein ausnahmsloses-Verbot der Verformelung und Speicherung von Analyseergebnissen, die inhaltliche Aussagen über Erbanlagen ermöglichen, ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkennt-

nisse, falls sich solche künftig aus der gespeicherten Verformelung der DNA ergeben sollten, die Begrenzung auf Personen, die wegen genau zu bestimmender schwerer Straftaten insbesondere gegen die körperliche Integrität und gegen die sexuelle Selbstbestimmung verurteilt und bei denen eine Wiederholungsgefahr festgestellt wurde, sofern die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

7.1.7.2 Das Strafverfahrensänderungsgesetz - DNA-Analyse ("genetischer Fingerabdruck") - (StVÄG)

Am 17.03.1997 hat der Bundestag in einem Strafverfahrensänderungsgesetz die Voraussetzungen und Grenzen molekulargenetischer Untersuchungen in einem konkreten Strafverfahren geregelt. Er hat klargestellt, daß **Blutproben und sonstige Körperzellen**, die dem Beschuldigten entnommen werden, nur für Zwecke des der Entnahme zugrundeliegenden oder eines anderen anhängigen Strafverfahrens verwendet werden dürfen. Sie müssen unverzüglich vernichtet werden, sobald sie hierfür nicht mehr erforderlich sind. Molekulargenetische Untersuchungen an diesem Material dürfen nur zur Feststellung, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt oder ob eine Person von einer anderen abstammt, durchgeführt werden. Weitere Feststellungen dürfen nicht erfolgen; hierauf gerichtete Untersuchungen sind unzulässig.

Das Gesetz enthält jedoch weder Vorschriften ob und in welchen Grenzen eine Speicherung und Nutzung der durch DNA-Analysen gewonnenen Untersuchungsergebnisse in zentralen Datenbanken der Polizei zulässig ist, noch sind darin Regelungen getroffen, die eine Erhebung ermöglichen, wenn eine DNA-Analyse z.B. wegen eines Geständnisses des Angeklagten für das Strafverfahren nicht erforderlich ist.

7.1.7.3 Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur Speicherung genetischer Informationen in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken

Wir Datenschutzbeauftragten des Bundes und der Länder haben schon in unserer 53. Konferenz eine Entschließung zur Speicherung genetischer Informationen in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken gefaßt ([Anlage 5](#)). Darin brachten wir bereits damals zum Ausdruck, daß wir derartige Speicherungen - eine ausreichende gesetzliche Regelung vorausgesetzt - **grundsätzlich für zulässig halten**. Wir haben aber darauf hingewiesen, daß hinsichtlich des Gefährdungspotentials der Analyseergebnisse ein grundsätzlich neuer Aspekt zu berücksichtigen ist.

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen nach derzeitigem Stand der Wissenschaft zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Anbetracht der weltweit intensiven Forschung im Bereich der Genomanalyse ist es jedoch nicht ausgeschlossen, daß künftig auch auf der Basis der bisherigen Untersuchungen konkrete Aussagen über genetische Dispositionen der betroffenen Personen getroffen werden können. Mit anderen Worten: Es besteht die Gefahr, daß aus den gespeicherten Informationen in Zukunft mehr herausgelesen werden kann, als zulässig ist.

Wir haben daher ein ausnahmsloses Verbot der Speicherung und Nutzung solcher Analyseergebnisse gefordert, die inhaltliche Aussagen über Erbanlagen ermöglichen.

Weiter haben wir gefordert, daß nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, in eine zentrale Datei aufgenommen werden darf. Es müssen tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird **und** daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Wir haben deshalb schließlich gefordert, die Daten dieser Personen unmittelbar dann zu löschen, wenn sie für

das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

7.1.7.4 Errichtung einer zentralen DNA-Analyse-Datei

Fast ein Jahr lang seit dieser Entschließung geschah gar nichts. Dann überschlugen sich die Ereignisse. Zunächst wurde ein **Arbeitsentwurf des Bundesministers der Justiz** zur Errichtung einer DNA-Analyse-Datei beim Generalbundesanwalt vorgelegt.

Dieser Entwurf erfüllte im wesentlichen die Voraussetzungen, die die 53. Konferenz der Datenschutzbeauftragten in der oben beschriebenen Entschließung aufgestellt hatte.

Zu diesem Entwurf hat mir das Staatsministerium der Justiz keine Gelegenheit zur Stellungnahme gegeben. Es hat einen eigenen **Gesetzesentwurf zur Änderung des § 81 b StPO** (erkennungsdienstliche Behandlung) vorgelegt, der eine DNA-Analyse zu erkennungsdienstlichen Zwecken, aber keine besondere gesetzliche Grundlage für die Errichtung einer Datei vorsah. Die Grundgedanken dieses Entwurfs fanden Eingang in das inzwischen in Kraft getretene DNA-Identitätsfeststellungsgesetz. Ich gehe deswegen hier näher auf ihn ein.

Ich habe zunächst gegenüber dem Justizministerium darauf hingewiesen, daß aus datenschutzrechtlicher Sicht gegen die Einrichtung einer bundesweiten DNA-Identifizierungs-Datei keine Bedenken bestehen, sofern die Mindestanforderungen erfüllt werden, die sich aus der oben beschriebenen Entschließung der 53. Konferenz der Datenschutzbeauftragten ergeben.

Das Fehlen einer besonderen gesetzlichen Grundlage für die Errichtung einer solchen Datei wird in folgenden Schwachpunkten des bayerischen Entwurfs deutlich, auf die ich das Justizministerium hingewiesen habe:

- Es war nicht sichergestellt, daß eine Speicherung und Nutzung, die Rückschlüsse auf persönlichkeitsrelevante Erkenntnisse zuläßt, ausgeschlossen ist.
- Es fehlten ausdrückliche Regelungen über die Dauer der Speicherungen sowie Vorschriften über die Löschung der gespeicherten Untersuchungsergebnisse.
- Es fehlte eine Regelung, die eine enge Zweckbindung gewährleistet. Auskünfte aus der

DNA-Datei sollten - so wie es der Vorschlag des Bundesjustizministers vorsah - nur Strafverfolgungsbehörden und Gerichte für Zwecke eines Strafverfahrens erhalten.

- Der Begriff der "Straftaten von erheblicher Bedeutung" war sehr unbestimmt. Besser wäre eine engere Eingrenzung gewesen z.B. durch einen Straftatenkatalog oder durch Regelbeispiele.

Unbeeindruckt vom Fehlen einer ausreichenden Rechtsgrundlage hatte der Bundesinnenminister die Errichtung einer zentralen DNA-Analyse-Datei beim Bundeskriminalamt forciert. Das Staatsministerium des Innern hatte es leider unterlassen, mir zu dem entsprechenden Entwurf **der Errichtungsanordnung** Gelegenheit zur Stellungnahme zu geben. Ich hätte eine solche vorherige Beteiligung angesichts der erheblichen datenschutzrechtlichen Bedeutung dieser Errichtungsanordnung begrüßt.

Kurz vor der Sommerpause haben die Fraktionen der CDU/CSU und F.D.P. einen neuen **Entwurf eines Gesetzes zur Änderung der Strafprozeßordnung (DNA-Identitätsfeststellungsgesetz)** eingebracht. Darin war eine Ergänzung der Strafprozeßordnung zur Regelung der Entnahme von Körperzellen beim Beschuldigten und beim bereits Verurteilten zur Durchführung molekulargenetischer Untersuchungen für Zwecke der Identitätsfeststellung in künftigen Strafverfahren vorgesehen.

Eine bereichsspezifische gesetzliche Grundlage für eine zentrale DNA-Analyse-Datei fehlte auch hier, sieht man von der unzureichenden Verweisung auf die Verarbeitungs- und Nutzungsregelungen des Bundeskriminalamtsgesetzes ab.

Ich habe Regelungen gefordert, wonach die gespeicherten Untersuchungsergebnisse ausschließlich zur Verfolgung von Straftaten und zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit verwendet werden dürfen (enge Zweckbindung). Ich habe gerügt, daß der Richtervorbehalt nicht konsequent umgesetzt werden soll. Nach meiner Auffassung bedarf es in jedem Fall einer Prognoseentscheidung des Richters zur Wiederholungsgefahr, wenn der "genetische Fingerabdruck" auf Dauer gespeichert werden soll. Darüber hinaus halte ich es auch für notwendig, daß sichergestellt ist, daß genetische Daten von unbeteiligten Personen, die freiwillig an Speicheltests (DNA-Screening) teilnehmen, nicht in der Datei gespeichert und abgeglichen werden können.

Trotz dieser auch öffentlichen Appelle wurde das Gesetz im wesentlichen unverändert beschlos-

sen. Es ist am 11.09.1998 in Kraft getreten.

7.2 Automatisierte Datenverarbeitungsverfahren bei der Justiz

7.2.1 Geschäftsstellenautomationsverfahren für Staatsanwaltschaften SIJUS-Straf-StA

In meinem 15. Tätigkeitsbericht (Nr. 6.4.1) sowie in meinem 17. Tätigkeitsbericht ([Nr. 7.2.1](#)) habe ich über das nunmehr bei allen bayerischen Staatsanwaltschaften eingesetzte Geschäftsstellensystem für Staatsanwaltschaften SIJUS-Straf-StA berichtet.

Im Berichtszeitraum habe ich zwei Staatsanwaltschaften geprüft und dabei die Einhaltung datenschutzrechtlicher Vorgaben in der Praxis überprüft. Darüber hinaus hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Thema "Datenschutzrechtliche Forderungen zum Einsatz von staatsanwaltschaftlichen Informationssystemen" befaßt und ein entsprechendes Thesenpapier grundsätzlich zustimmend zur Kenntnis genommen.

7.2.1.1 Ergebnisse der rechtlichen Prüfungen

- **Erfassung der Postanschrift**

Nach der Dienstanweisung SIJUS-Straf-StA vom 13.09.1996 sind bei der Erfassung der Postanschrift ergänzende Hinweise, die darauf schließen lassen, daß sich der Empfänger in einer Justizvollzugsanstalt aufhält, zu unterlassen. Eine Verwendung solcher Zusätze konnte bei einer Staatsanwaltschaft in zwei Fällen festgestellt werden, wobei sich der eine Zusatz auf die Zeit vor Inkrafttreten der Dienstanweisung bezieht, der andere auf die Zeit danach. Ich habe dies angesichts der Vielzahl gespeicherter Datensätze als offensichtliche Ausreißer bewertet. Die Zusätze wurden gelöscht und die betreffende Erfasserkraft auf die Unzulässigkeit derartiger Zusätze hingewiesen.

- **Berichtigung des Tatvorwurfs**

Die Dienstanweisung SIJUS-Straf-StA sieht vor, die ursprüngliche Bezeichnung des Tat-

vorwurfs unverzüglich, spätestens zum Zeitpunkt der staatsanwaltschaftlichen Verfahrenserledigung zu berichtigen, wenn sich der Tatverdacht wesentlich ändert.

Bei einer der von mir geprüften Staatsanwaltschaften wurde das Formblatt für die Anklageerhebung deshalb um den Punkt "Tatbezeichnung umändern" ergänzt. Ich halte dies für vorteilhaft, da dadurch an die Notwendigkeit einer entsprechenden Prüfung erinnert wird. Ich habe beim Staatsministerium der Justiz angeregt, dieses Verfahren für alle Staatsanwaltschaften vorzuschreiben.

Stichprobenartige Überprüfungen aus den Deliktsbereichen Totschlag, Vergewaltigung, räuberischer Diebstahl und räuberische Erpressung mit dem Ziel festzustellen, ob der richtige Tatvorwurf in SIJUS-Straf-StA gespeichert ist, ergab bei beiden von mir geprüften Staatsanwaltschaften jeweils nur ein Verfahren, bei dem die notwendige Berichtigung übersehen worden war. In beiden Verfahren wurde der Tatvorwurf nachträglich berichtigt.

- **Datensperre bei Verfahrenseinstellung wegen Wegfall des Tatverdachts**

Nach der Dienstanweisung SIJUS-Straf-StA ist eine Datensperre zwingend vorzunehmen, wenn ein Verfahren eingestellt wurde und kein begründeter Verdacht mehr besteht. Der Behördenleiter bestimmt durch schriftliche Anordnung, wer die Datensperre veranlassen und auf gesperrte Eintragungen zugreifen kann, sowie wer im Verhinderungsfall vertretungsbefugt ist. Bei einer der von mir geprüften Staatsanwaltschaften lag eine schriftliche Anordnung des Behördenleiters nicht vor. Sie wurde zwischenzeitlich erlassen.

- **Löschung von Altverfahren**

Nach den Aufbewahrungsbestimmungen sind nach § 170 Abs. 2 StPO eingestellte Verfahren nach 5 Jahren auszusondern und zu vernichten. In der Dienstanweisung SIJUS-Straf-StA ist vorgesehen, daß die gespeicherten Personen- und Verfahrensdaten mit Ab-

lauf der Aufbewahrungsfristen taggenau vollständig gelöscht werden. Bei der Prüfung einer Staatsanwaltschaft mußte ich feststellen, daß bislang eine automatische Löschung der gespeicherten Daten in SIJUS-Straf-StA mangels erforderlicher Softwarefunktionen noch nicht möglich war.

Das Staatsministerium der Justiz hat dies bestätigt und mitgeteilt, daß diese Funktion im Zeitpunkt der Prüfung lediglich bei einer Staatsanwaltschaft möglich war. Zwischenzeitlich steht die Funktion - wie ich bei meiner weiteren Prüfung feststellen konnte - allgemein zur Verfügung.

7.2.1.2 Datenschutzrechtliche Forderungen zu staatsanwaltschaftlichen Informationssystemen

Aus den von der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder grundsätzlich zustimmend zur Kenntnis genommenen Thesen zu Anforderungen an staatsanwaltschaftliche Informationssysteme habe ich für Bayern die folgenden Forderungen abgeleitet, die aus meiner Sicht noch nicht oder nur unzureichend berücksichtigt sind:

- **Löschungsfristen:**

Konkrete Löschungsfristen, die sich am jeweiligen Zweck der Speicherung zu orientieren haben (laufende Strafverfahren, Strafvollstreckung, künftige Strafverfahren, Vorgangsverwaltung) sollten vorgesehen werden. Sobald die Daten von Hauptbeteiligten (z.B. Mitbeschuldigten) nicht mehr für das Strafverfahren benötigt werden, ist eine Teillöschung der Daten vorzunehmen. Dabei ist der Zeitpunkt der Teillöschung für jeden Hauptbeteiligten individuell zu bestimmen.

- **Zugriffsbeschränkungen und Datenspernung:**

Werden Daten eines Ermittlungsverfahrens in automatisierten staatsanwaltschaftlichen Informationssystemen für andere Stellen (z.B. Bewährungshelfer) abrufbar bei der bearbeitenden Staatsanwaltschaft gespeichert, ist der Zugriff auf diese Daten auf das für die

jeweilige Aufgabenerfüllung der abrufenden Stelle erforderliche Maß zu beschränken.

Eine geeignete Maßnahme zur Beschränkung des internen Zugriffs ist die Vergabe differenzierter Zugriffsrechte. Sie muß systemseitig ermöglicht werden. Über die genaue Vergabe von Zugriffsrechten kann keine allgemein gültige Aussage getroffen werden, da die jeweiligen Organisationsformen der Staatsanwaltschaften berücksichtigt werden müssen. Zugriffsbeschränkungen können z.B. beim datenverändernden Zugriff, beim lesenden Zugriff sowie beim Kreis der Zugriffsberechtigten in Abhängigkeit vom Verfahrensstand und von der Art der Daten einsetzen.

- **Vergabe und Dokumentation von Zugriffsrechten:**

Die Vergabe von Zugriffs- und Bearbeitungsrechten sowie deren Änderung, Sperrung oder Löschung ist revisionsfähig zu dokumentieren. Im Datenschutzkonzept der Anwender ist festzulegen, auf welche Art und Weise und durch wen die Vergabe und Dokumentation dieser Rechte erfolgt.

- **Protokollierung:**

Das Ändern, Sperren und Löschen der Daten ist in jedem Fall zu protokollieren. Nicht ausreichend ist die Protokollierung lediglich des jeweils letzten Zugriffs auf einen Datensatz.

Alle Aktivitäten, die der Systemverwaltung dienen, sollten revisionssicher aufgezeichnet werden.

Die Aufbewahrung der Protokolldaten sollte über einen angemessenen Zeitraum hinweg erfolgen. Die Nutzung der Protokolldaten z.B. für Zwecke der Datenschutzkontrolle oder zur Sicherung eines ordnungsgemäßen Betriebes der DV-Anlage ist vorher festzulegen. Dabei ist eine enge Zweckbindung sicherzustellen. Um eine verbotswidrige Auswertung der Protokolldaten zu vermeiden, sollte soweit möglich das "Vier-Augen-Prinzip" ge-

währleistet werden.

- **Datenaustausch mit anderen Stellen:**

Der Datenaustausch (Übermittlung und Abruf) mit dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) und dem Bundeszentralregister (BZR) und anderen speichernden Stellen wie z.B. Gerichten, Strafvollzugsbehörden oder Polizei sollte grundsätzlich nur im Rahmen von Verfahren abgewickelt werden, die durch Einsatz geeigneter kryptographischer Verfahren (z.B. Verschlüsselung, digitale Signatur) die Vertraulichkeit, Integrität und Zurechenbarkeit der Daten sicherstellen. Kommen Abrufverfahren zum Einsatz, so sind sowohl auf den Übertragungswegen als auch bei den abrufenden Stellen Vorkehrungen zu treffen, damit das interne Sicherheitsniveau der staatsanwaltschaftlichen Systeme erhalten bleibt.

Das staatsanwaltschaftliche Informationssystem sollte darüber hinaus gewährleisten, daß die Polizei sowohl über die Berichtigung des Tatvorwurfs wie auch über den Ausgang des Verfahrens möglichst umgehend informiert wird, soweit sie mit der Angelegenheit befaßt war.

- **Einsatz von PC:**

Der Einsatz von PC bedingt Datensicherheitsprobleme. Es sind daher Maßnahmen zu treffen, die einen Im- und Export von Daten über ungesicherte Schnittstellen und Laufwerke, eine unerlaubte Weiterverarbeitung mittels Standardsoftware und einen unerlaubten Zugriff auf die Systemebene verhindern. Soweit bei den PC die Diskettenlaufwerke nicht gesperrt werden können, sind besondere Sicherheitsmaßnahmen, wie z.B. die verschlüsselte Speicherung vorzusehen. Sonstige nicht benötigte Schnittstellen sind zu sperren.

Im übrigen sollten

- der lesende Zugriff zumindest stichprobenartig protokolliert werden; dies gilt ins-

besondere im Hinblick auf die landesweite Abfragemöglichkeit,

- vergebliche Zugriffsversuche auf die Betriebssystemebenen protokolliert werden, um ggf. Mißbrauchsversuchen nachgehen zu können,
- in der Dienstanweisung zu SIJUS-Straf-StA eine Sperrung von Daten vorgesehen werden, wenn der Beschuldigte rechtskräftig freigesprochen oder die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt worden ist.

Das Staatsministerium der Justiz hat die Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz mit diesen Forderungen befaßt. Diese hat die Einrichtung einer Arbeitsgruppe beschlossen, die die von den Datenschutzbeauftragten erhobenen Forderungen aus Sicht der Justiz bewerten soll.

Ein Ergebnis steht noch aus.

7.2.2 Aufbau eines zentralen staatsanwaltschaftlichen Verfahrensregisters in Bayern (STARIS)

In meinem 17. Tätigkeitsbericht ([Nr. 7.2.2](#)) habe ich über den damaligen Stand der Realisierung eines landesweiten Verfahrensregisters in Bayern berichtet. Ich habe ferner deutlich gemacht, daß ich von einer förmlichen Beanstandung dieses ohne Rechtsgrundlage eingeführten Verfahrens im Echtbetrieb nur dann absehen werde, soweit Art und Umfang der in STARIS gespeicherten personenbezogenen Daten und die Auswertungsmöglichkeiten in diesem System nicht über das bundesweite staatsanwaltliche Informationssystem (ZStV) hinausgehen.

Inzwischen ist die Entwicklung von STARIS weitgehend abgeschlossen. Seit Dezember 1997 sind alle bayerischen Staatsanwaltschaften angeschlossen. Derzeit werden in STARIS die aus der Praxis gemeldeten Fehler bearbeitet, Ergänzungen realisiert und das Programm an die für Januar 1999 vorgesehene neue Version des staatsanwaltschaftlichen Informationssystems SIJUS-Straf-StA angepaßt.

Die für die Freigabe von STARIS erforderliche Verfahrensbeschreibung steht noch aus. Das Staatsministerium der Justiz hat angekündigt, diese demnächst, gleichzeitig mit einer entsprechenden Dienstanweisung zu erlassen.

Das Staatsministerium der Justiz hat bestätigt, daß die **Löschung** von Daten in STARIS - wie im ZStV - innerhalb einer Frist von 2 Jahren nach Erledigung des Verfahrens erfolgt, wenn der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wurde. Die erste Löschung ist für Mitte Oktober 1998 vorgesehen.

Eine Speicherung von **Bußgeldverfahren** in STARIS erfolgt derzeit nicht und wird nach Aussage des Staatsministeriums der Justiz auch künftig nicht erfolgen.

Soweit bei der Mitteilung eines Beschuldigten an STARIS eine Auskunft über solche Personen erscheint, bei denen der Grad der Übereinstimmung nicht zur Feststellung der Identität mit bereits gespeicherten Personen ausreicht, obwohl die Wahrscheinlichkeit einer Identität sehr hoch ist, werden die entsprechenden Daten in der EDV der Staatsanwaltschaft nicht gespeichert, sondern nur in einer Vorgangsliste ausgegeben. Diese ist kein Bestandteil der Akten sondern wird zu den Handakten genommen und ist damit nur für den Sachbearbeiter des konkreten Verfahrens zugänglich. Das Justizministerium hat in Aussicht gestellt, daß die Dienstanweisung für STARIS eine Vernichtung dieser Unterlagen zu dem Zeitpunkt vorsehen wird, in dem der Sachbearbeiter entscheidet, daß zwischen der mitgeteilten **ähnlichen Person** und dem Beschuldigten keine Identität besteht.

Anläßlich der Prüfung einer Staatsanwaltschaft im Berichtszeitraum habe ich festgestellt, daß die aus STARIS abrufbaren Daten den Umfang nicht überschreiten, der von der Strafprozeßordnung für das bundesweite zentrale staatsanwaltschaftliche Verfahrensregister (ZStV) vorgesehen ist. Ich werde in nächster Zeit die Einhaltung der Vorgaben für STARIS in der Praxis überprüfen. Darin werde ich die Frage einbeziehen, ob dieses System nach Inbetriebnahme des zentralen staatsanwaltschaftlichen Verfahrensregisters (ZStV) angesichts des nahezu gleichen Datensatzes überhaupt noch erforderlich ist.

7.2.3 Aufbau eines zentralen staatsanwaltschaftlichen Verfahrensregisters auf Bundesebene (ZStV)

In meinem 16. Tätigkeitsbericht ([Nr. 7.2.2](#)) habe ich über das mit dem Verbrechensbekämpfungsgesetz geschaffene staatsanwaltschaftliche Verfahrensregister beim Bundeszentralregister berichtet. Der Sachstand stellt sich aktuell wie folgt dar:

Die Inbetriebnahme des ZStV soll planmäßig zum 01.01.1999 erfolgen. Ebenfalls für Anfang 1999 wird die Anbindung der bayerischen Staatsanwaltschaften an das ZStV angestrebt. Bis dahin muß allerdings das Datenverarbeitungssystem SIJUS-Straf-StA programmtechnisch angepaßt werden.

Das Sicherheitskonzept als Teil der aufgrund der Errichtungsanordnung erlassenen technisch-organisatorischen Leitlinien des ZStV sieht grundsätzlich eine Verschlüsselung bei der Datenübertragung vor. Es ist allerdings damit zu rechnen, daß für eine Übergangsphase Datenübermittlungen ohne Verschlüsselung vorgenommen werden, da erst der laufende Pilotierungsversuch der Koordinierungs- und Beratungsstelle der Bundesregierung für IT in der Bundesverwaltung beim Bundesinnenministerium die grundsätzliche Eignung des vorgesehenen Verschlüsselungsverfahrens für das ZStV erproben will.

7.2.4 Automation der Aufgaben der Vollzugsgeschäftsstelle und Einrichtung eines Informationssystems über Gefangenendaten (ADV-Vollzug)

Derzeit entwickelt die Justiz ein Verfahren zur Automation der Aufgaben der Vollzugsgeschäftsstelle und der Einrichtung eines Informationssystems über Gefangenendaten. Das Verfahren umfaßt zunächst Personal, Vollstreckungs- und Termindaten. Die Daten des bisherigen Personalblatts (A-Bogen) werden erfaßt und gepflegt; Übersichten und Statistiken aus dem vorhandenen Datenbestand sollen ermöglicht werden. So ist es beispielsweise möglich, eine Liste aller Gefangenen mit sogenannten "Sicherheitsvermerken" auszudrucken. Daneben sind Programme vorgesehen, die die Verwaltung der Termine des Vollzugsplans, der Vollzugsformen, von Arbeitszuweisungen, besonderer Sicherungsmaßnahmen, von Abwesenheiten, von Lockerungsvorgaben oder Disziplinarmaßnahmen sowie von Besuchsdaten ermöglichen.

Das System wurde zunächst in einer Justizvollzugsanstalt erprobt, der Probetrieb sodann auf zwei weitere Justizvollzugsanstalten ausgedehnt. Wann die Erprobungsphase abgeschlossen sein wird, ist derzeit noch nicht absehbar.

Ich habe mich zunächst wegen der folgenden Punkte an das Staatsministerium der Justiz gewandt:

1. Differenzierte Zugriffsrechte

Ich habe begrüßt, daß die Entwicklung eines schlüssigen Konzeptes zur Steuerung der Zugriffsrechte beabsichtigt ist. Ich habe darauf hingewiesen, daß ich davon ausgehe, daß damit ein Zugriff der Bediensteten nur auf diejenigen Daten möglich sein wird, die diese zu ihrer konkreten Aufgabenerfüllung auch tatsächlich benötigen. Zum Beispiel sind Sicherheitsvermerke wie "Gefahr des Angriffs von Bediensteten" und "Gefahr der Geiselnahme" sowie "Ansteckungsgefahr" für alle Vollzugsbediensteten von Bedeutung, während andere (z.B. "Lockerungsversager", "Alkoholiker", "nur Einzelunterbringung") nur für die Aufgabenerfüllung einiger Bediensteter relevant sind.

2. Kontinuierliche Datenlöschung

Ich habe darauf hingewiesen, daß nach Entlassung des Gefangenen nur noch eine elektronische Speicherung derjenigen Daten erforderlich und damit zulässig sein kann, die ein Auffinden der Akten ermöglichen. Daher sollte möglichst automatisch der Datenbestand entsprechend reduziert werden.

Zwischenzeitlich ist die Löschung von Gefangenendaten gesetzlich geregelt. Danach sind die in Daten gespeicherten personenbezogenen Daten spätestens zwei Jahre nach der Entlassung des Gefangenen oder der Verlegung des Gefangenen in eine andere Anstalt zu löschen. Hiervon können bis zum Ablauf der Aufbewahrungsfrist für die Gefangenepersonalakte die Angaben über Name, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum des Gefangenen ausgenommen werden, soweit dies für das Auffinden der Gefangenepersonalakte erforderlich ist.

Das Staatsministerium der Justiz hat zugesagt, daß bei Einführung des automatisierten Verfah-

rens zur Erledigung der Geschäfte der Vollzugsstelle in der jeweiligen Anstalt geprüft werden wird, welche Daten zielgerichtet und bedarfsgerecht an den einzelnen Bediensteten zur Erfüllung seiner konkreten Aufgaben über den Bildschirmarbeitsplatz weitergegeben werden können.

7.2.5 Automatisiertes gerichtliches Mahnverfahren (AUGEMA)

Derzeit wird das automatisierte gerichtliche Mahnverfahren in Bayern lediglich beim Amtsgericht München für den Bezirk dieses Gerichts, bei dem Amtsgericht Nürnberg für die Bezirke der Amtsgerichte Nürnberg und Fürth sowie beim Amtsgericht Coburg für die Bezirke der Amtsgerichte Coburg und Lichtenfels eingesetzt. Das Verfahren ist auf wenige Großgläubiger beschränkt, die am Datenträgeraustausch teilnehmen.

Im Rahmen dieses Verfahrens werden Arbeiten von zwei Privatfirmen aus Nürnberg und Weiden durchgeführt. Diese erfassen die in Rücklauf kommenden **Postzustellungsurkunden**. Dabei ist vertraglich vereinbart, daß die betreffenden Firmen die notwendigen technischen und organisatorischen Maßnahmen treffen.

Es ist beabsichtigt, das automatisierte Mahnverfahren schrittweise zu zentralisieren und auch die bislang in Papierform eingereichten **Mahnbescheidsanträge** durch Fremdfirmen erfassen zu lassen.

Das Amtsgericht Coburg soll langfristig die zentrale Zuständigkeit für das Mahnverfahren in Bayern erhalten. Dort soll zunächst ein zentrales Mahngericht für die Oberlandesgerichtsbezirke Nürnberg und Bamberg eingerichtet und später auch die Bearbeitung der Mahnsachen des Oberlandesgerichtsbezirks München nach Coburg verlagert werden.

Ich habe gegenüber dem Staatsministerium der Justiz darauf hingewiesen, daß ich die Verlagerung reiner Hilfstätigkeiten auf Private auch im Rahmen des gerichtlichen Mahnverfahrens unter bestimmten Voraussetzungen für zulässig halte.

Insbesondere sind die Vorschriften einzuhalten, die für Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag gelten ([Art. 6 BayDSG](#)). Danach bleibt der Auftraggeber datenschutzrechtlich für alle Maßnahmen verantwortlich. Er hat die Auftragnehmer unter besonderer Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen auszuwählen und dem Umfang der Arbeiten in Bezug auf die zu erhebenden personenbezo-

genen Daten exakt festzulegen. Auch Löschungspflichten sind schriftlich zu fixieren.

Darüber hinaus ist sicherzustellen, daß das Bayerische Datenschutzgesetz für den Auftragnehmer Anwendung findet und daß sich dieser einem anlaßunabhängigen **Kontrollrecht** des Landesbeauftragten für den Datenschutz unterwirft.

Ferner sollten bei Verstößen gegen den Datenschutz eine Vertragsstrafe und für geeignete Fälle ein Recht auf fristlose Kündigung vereinbart werden.

Schließlich muß sichergestellt sein, daß das mit der Datenverarbeitung befaßte Personal nach dem Verpflichtungsgesetz verpflichtet wird, und Unterauftragsverhältnisse vertraglich ausgeschlossen werden. Es sollte möglichst nur zuverlässiges Stammpersonal eingesetzt werden.

Ich habe festgestellt, daß diese Forderungen, von einigen Ausnahmen abgesehen, in dem mir vom Staatsministerium der Justiz vorgelegten Vertragsmuster berücksichtigt sind.

Folgende Punkte müssen noch ergänzt werden:

- Festlegung, welche Sicherungsmaßnahmen (z.B. Verschlüsselung) bei einer Datenfernübertragung einzuhalten sind,
- Konkretisierung der erforderlichen Maßnahmen nach [Art. 6 Abs. 2 BayDSG](#),
- Vereinbarung eines Rechts auf fristlose Kündigung,
- Zugang kontrollierender Personen nicht nur zum Datenerfassungsraum sondern auch zum Rechnerraum und dem Raum bzw. Schrank, in welchem die Magnetbänder aufbewahrt werden,
- Erweiterung des Zugangs- und Auskunftsrechts für den Landesbeauftragten für den Datenschutz in ein Kontrollrecht,

Auch wenn die Daten der eingereichten Anträge auf Erlaß eines Mahn- und Vollstreckungsbescheids im Vergleich zu den Daten aus Postzustellungsurkunden ungleich sensibler sind, halte ich die geplante Ausweitung der Erfassungsarbeiten unter den vorgenannten Voraussetzungen für vertretbar. Ich habe aber deutlich gemacht, daß allein die Verpflichtung des Auftragnehmers, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, für sich allein nicht

ausreicht. Da der Auftraggeber nach [Art. 6 Abs. 1 BayDSG](#) für die Einhaltung der Vorschriften über den Datenschutz verantwortlich bleibt, muß er in der Lage sein, die getroffenen technischen und organisatorischen Datenschutzmaßnahmen zu überprüfen und bei Bedarf zusätzliche Maßnahmen zu verlangen.

7.3 Datenschutz bei der Strafverfolgung

7.3.1 Öffentlichkeitsfahndung im Internet

Ende 1996 hat die bayerische Polizei begonnen, Fahndungsaufrufe im Internet zum Abruf bereitzuhalten. Die Fahndungsaufrufe, die zunächst unter der Bezeichnung "Bayerns Meistgesuchte" veröffentlicht wurden, enthalten ein Bild des Betroffenen, seine Personalien sowie eine Kurzbeschreibung persönlicher Merkmale wie Haarfarbe, Augenfarbe und Geschlecht. Es folgt eine Kurzschilderung des Fahndungsgrundes und die Angabe der zuständigen Polizeidienststelle. In den ersten zweieinhalb Monaten seit Einrichtung dieser Fahndungsseiten wurde eine Million mal im World Wide Web auf das Angebot der bayerischen Polizei zugegriffen, wovon fast die Hälfte der Zugriffe, nämlich 44 %, aus dem nicht deutschsprachigen Raum stammt. Dabei fanden die Fahndungsseiten mit 50 % aller Abrufe weltweit das größte Interesse. Gleichwohl sind Erfolge der bayerischen Polizei bislang nicht bekannt geworden.

Nach längerem Schriftwechsel mit dem Staatsministerium des Innern, in dem ich auch auf die Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur Öffentlichkeitsfahndung im Strafverfahren vom 14./15.03.1996 ([Anlage 2](#)) Bezug genommen und insbesondere darauf hingewiesen habe, daß derzeit weder für die Öffentlichkeitsfahndung noch speziell für die Internetfahndung eine ausreichende Rechtsgrundlage besteht, hat das Innenministerium die Bezeichnung "Bayerns Meistgesuchte" in "Mit Haftbefehl gesucht" geändert. Im übrigen konnte eine übereinstimmende Beurteilung der Voraussetzungen dieser Fahndungsmaßnahme nur teilweise erreicht werden. Nach meiner Auffassung ist die Fahndung im Internet - jedenfalls wenn sie wie bei den bayerischen Fahndungsaufrufen nicht nur in deutscher Sprache sondern zusätzlich in englisch, also einer weltweit verbreiteten Sprache erfolgt - weltweite Fahndung. Das bedeutet, daß zusätzlich zu den allgemeinen Voraussetzungen für eine Fahndung in der Öffentlichkeit in der Regel die Voraussetzungen einer internationalen Fahndung gegeben sein müssen. Ich habe deshalb bis zu einer gesetzlichen Regelung folgendes gefordert:

- Es müssen Anhaltspunkte dafür vorliegen, daß sich die gesuchte Person im Ausland befindet. Der konkrete Aufenthaltsort darf aber wegen des grundsätzlichen Vorrangs der örtlichen Fahndung nicht bekannt sein.
- Eine Auslieferung muß rechtlich zulässig sein. Es muß ernsthaft beabsichtigt sein, ein Auslieferungsersuchen zu stellen.
- Bei der Fahndung nach einem Beschuldigten muß ein Haftbefehl wegen des dringenden Verdachts eines Verbrechens oder einer anderen Straftat von erheblicher Bedeutung vorliegen.

Auch wenn keine Anhaltspunkte dafür vorliegen, daß sich die gesuchte Person im Ausland befindet, kommt eine Fahndung im Internet in Betracht, wenn wegen einer Straftat gegen das Leben oder wegen einer schwerwiegenden Straftat gegen die körperliche Unversehrtheit oder die persönliche Freiheit gefahndet werden soll und konkrete Anhaltspunkte für die Begehung weiterer gleichartiger Straftaten durch den Betroffenen vorliegen.

Das Staatsministerium des Innern teilt insbesondere nicht meine Auffassung, daß Öffentlichkeitsfahndungen im Internet eine andere Eingriffsqualität zukommt, als Fahndungsaufrufen in Funk, Fernsehen oder in den Printmedien.

Ich halte meine Auffassung aufrecht.

Fahndungsaufrufe in Funk und Fernsehen sind grundsätzlich auf den Sendezeitpunkt beschränkt und werden eher zufällig empfangen. Eine ins Internet eingestellte Fahndungsseite, die von anderen Usern kopiert und weiterverbreitet werden kann, kann auf der ganzen Welt gezielt abgerufen werden und steht unter Umständen noch Jahre später als "Fahndung" zur Verfügung. Hierdurch kann auch nach Abschluß des Verfahrens immer noch der Eindruck entstehen, eine Fahndung dauere noch an. Dies ist für den Betroffenen insbesondere dann besonders belastend, wenn sich seine Unschuld herausstellt. Im Gegensatz dazu läßt bei den Printmedien die Aktualität von Fahndungsaufrufen schnell nach. Sie werden schon nach kurzer Zeit, meist schon mit dem Erscheinen der neuen Ausgabe nicht mehr als Fahndung wahrgenommen.

Internetfahndung hat deshalb eine qualitativ höhere Eingriffsqualität als Fahndung in Funk, Fernsehen oder Printmedien.

Bei Fahndung im Internet muß im übrigen die Authentizität des Fahndungsaufrufs gewährleistet

sein. Durch geeignete technische Maßnahmen ist sicherzustellen, daß unberechtigte Veränderungen der Fahndungsaufrufe in der Homepage der Polizei ausgeschlossen sind. Aus der Homepage kopierte Fahndungsaufrufe, die von Dritten im Internet publiziert werden, sind durch geeignete technische Maßnahmen gegen Manipulationen zu schützen (z.B. durch Angabe eines Gültigkeitszeitraums oder eine digitale Signatur).

Die Fahndung im Internet stellt einen erheblichen Eingriff in das Persönlichkeitsrecht des Betroffenen (Beschuldigter/Zeuge) dar. Es sollte deshalb zum Zwecke einer Erfolgskontrolle der neuen Fahndungsmaßnahme die Zahl der eingegangenen Hinweise und der aufgrund dieser Hinweise ermittelten Personen erfaßt werden.

Inzwischen hat das Staatsministerium des Innern die Nutzung des Internet durch die Polizei neu geregelt und klar zum Ausdruck gebracht, daß es sich bei der Internetfahndung um eine Sonderform der Öffentlichkeitsfahndung handelt und deshalb alle Anforderungen gelten, die für eine Öffentlichkeitsfahndung vorliegen müssen. Danach ist insbesondere der Grundsatz der Verhältnismäßigkeit zu beachten. Das Internet dürfte nur dann für die Fahndung genutzt werden, wenn andere, den Betroffenen weniger beeinträchtigende Fahndungsmittel nicht erfolgversprechend erscheinen und die Inanspruchnahme des Fahndungsmittels nicht außer Verhältnis zur Bedeutung der Sache steht, also in der Regel nur bei Straftaten von erheblicher Bedeutung. Ferner sei anzustreben, daß bei der Fahndung nach bekannten Straftätern ein internationaler Haftbefehl vorliegt.

Diese Neuregelung wird im Ergebnis meinen rechtlichen Forderungen weitgehend gerecht. Dies hat auch meine erneute Überprüfung des Fahndungsbestandes im Juli 1998 ergeben.

7.3.2 Täter-Opfer-Ausgleich bei Erwachsenen

Aufgrund eines Informationsbesuches bei einer Staatsanwaltschaft und einer Eingabe habe ich mich mit den datenschutzrechtlichen Aspekten des Täter-Opfer-Ausgleichs bei Erwachsenen befaßt.

Nach der Legaldefinition ist Täter-Opfer-Ausgleich (TOA) das Bemühen des Täters, einen Ausgleich mit dem Verletzten zu erreichen. Auf welche Weise der Täter den Ausgleich mit dem Opfer herstellt, ist im Gesetz nicht geregelt, insbesondere ist dort nicht vorgesehen, daß dies auch

unter Einschaltung dritter Stellen geschehen kann. Der zuständige Referent der Staatsanwaltschaft entscheidet über die Geeignetheit des Falles und leitet ggf. die Akte mit regelmäßig besonders sensiblen personenbezogenen Daten an die Gerichtshilfe oder häufiger an **freie Träger** zur Durchführung des TOA weiter. Von dort wird der Täter mit der Bitte um Kontaktaufnahme unter Erläuterung von Sinn und Zweck des TOA angeschrieben. Wenn keine Bereitschaft des Täters besteht, am TOA mitzuwirken, wird die Akte an die Staatsanwaltschaft zurückgegeben; das Verfahren nimmt seinen normalen Gang. Stimmt der Täter zu, wird das Opfer informiert und befragt, ob Interesse an der Durchführung eines TOA besteht. Bei Zustimmung durch das Opfer erfolgt eine schriftliche Vereinbarung oder ein Ausgleichsgespräch. Die Akten werden sodann an die Staatsanwaltschaft zurückgegeben, dort wird das Verfahren abgeschlossen.

Dieser Ablauf führt regelmäßig zu einer Datenübermittlung an eine externe Stelle und zwar zu einem Zeitpunkt, an dem noch nicht klar ist, ob es zur Durchführung des TOA überhaupt kommen wird. Das Staatsministerium der Justiz hält eine Befugnis der Datenübermittlung an eine private Stelle auf der Grundlage des Bayerischen Datenschutzgesetzes zur Strafverfolgung für gegeben. Ich habe demgegenüber darauf hingewiesen, daß das Gesetz eine Datenübermittlung nur erlaubt, wenn sie **erforderlich** ist. Für erforderlich zu Zwecken des TOA halte ich eine Übermittlung von Daten aber nur dann, wenn ein TOA auch tatsächlich in Betracht kommt. Dies setzt grundsätzlich sowohl die Einwilligung des Täters als auch des Opfers zur Durchführung des TOA voraus. Für eine Übermittlung personenbezogener Daten an eine nichtöffentliche Stelle zur Durchführung des TOA sollte deshalb die **vorherige Einwilligung** der Betroffenen vorliegen. Das Staatsministerium der Justiz vertritt hierzu die Auffassung, daß die Erforderlichkeit einer Datenübermittlung auch darin liegen kann, die Bereitschaft des Täters, am TOA mitzuwirken, durch eine besonders sachkundige Stelle zu wecken bzw. zu fördern. Erfahrungen in anderen Ländern haben in der Tat gezeigt, daß sich dadurch erheblich mehr Täter zur Mitwirkung bewegen lassen.

Im Hinblick darauf und auf den hohen Stellenwert des TOA, der vom Gesetzgeber im Jahre 1994 ausdrücklich in das Strafgesetzbuch aufgenommen wurde, würde ich folgendem Verfahren für eine Übergangszeit bis zur Schaffung einer bereichsspezifischen Regelung nicht entgegenreten, auch weil die Erstübermittlung weniger Daten im Interesse des Täters liegt und schutzwürdige Interessen am Ausschluß der Übermittlung in der Regel nicht bestehen dürften:

Die Staatsanwaltschaft übermittelt dem freien Träger zunächst Namen und Anschrift des Be-

schuldigten und eine kurze Schilderung des Sachverhaltes, damit dem freien Träger ermöglicht wird, die Bereitschaft des Täters, am TOA mitzuwirken, zu wecken. Dies gilt aber nicht für Daten des Opfers, weil bei diesem davon auszugehen ist, daß schutzwürdige Interessen einer Übermittlung entgegenstehen. Erklärt sich der Täter einverstanden, ist in jedem Fall vor der Übermittlung weiterer Daten das Einverständnis des Opfers durch die Staatsanwaltschaft einzuholen. **Akten** dürfen nur übersandt werden, wenn Täter und Opfer auch hiermit ausdrücklich einverstanden sind.

7.3.3 Verfahrensweise bei Einstellungen nach § 153 a stop

In meinem 17. Tätigkeitsbericht ([Nr. 7.6.6](#)) habe ich die Haltung des Staatsministeriums der Justiz zur Mitteilung personenbezogener Daten von Beschuldigten an gemeinnützige Einrichtungen, denen eine Geldauflage zugewiesen worden ist, geschildert.

Das Justizministerium hat meinen Vorschlag, bei Erholung der Zustimmung des Beschuldigten mit einer Sachbehandlung nach § 153 a StPO (Einstellung des Verfahrens bei Erfüllung von Auflagen und Weisungen) gleichzeitig dessen Einverständnis mit der Übermittlung seiner Daten an die Bußgeldempfänger zu erfragen und ihm bei fehlendem Einverständnis das Risiko einer rechtzeitigen und zuordenbaren Zahlung zuzuweisen, geprüft.

Der mir zugeleitete Entwurf eines EDV-geeigneten Vordrucks sah folgenden Hinweis an den Beschuldigten vor: "Die Zustimmung beinhaltet auch die Befugnis der Staatsanwaltschaft, beim Zahlungsempfänger die Erfüllung der Auflage zu überprüfen".

Gegen diese Formulierung habe ich Bedenken geäußert. Sie macht nach meiner Auffassung nicht hinreichend deutlich, daß zum Zwecke der Überprüfung auch personenbezogene Daten des Beschuldigten an den Zahlungsempfänger übermittelt werden sollen. Die Zustimmung zur Einstellung des Verfahrens gemäß § 153 a Abs. 1 StPO und die **datenschutzrechtliche Zustimmung** für die Übermittlung von Daten des Beschuldigten müssen deutlich unterschieden werden. Auch die Fälle, in denen ein Beschuldigter zwar der Einstellung nach § 153 a Abs. 1 StPO zustimmen, gegenüber dem Zahlungsempfänger aber anonym bleiben möchte, müssen umfaßt werden. Bei der vorgesehenen Formulierung bleibt dem Beschuldigten nur die Möglichkeit auf seine Zustimmung zur Verfahrenseinstellung zu verzichten oder, falls er dies nicht will, der Datenüber-

mittlung zuzustimmen. Ein solches Ergebnis erscheint mir nicht akzeptabel, da die Zustimmung zur Datenübermittlung nach § 153 a StPO keine Voraussetzung für die Einstellung des Verfahrens ist.

Ich habe deshalb vorgeschlagen, gleichzeitig mit Erholung des Einverständnisses des Beschuldigten mit einer Sachbehandlung nach § 153 a StPO auch dessen **ausdrückliche Zustimmung mit der Übermittlung** seiner personenbezogenen Daten an den Geldbußenempfänger zu erfragen.

Nach nochmaliger Erörterung auf einer Dienstbesprechung mit den Leiterinnen und Leitern der bayerischen Staatsanwaltschaften hat das Staatsministerium der Justiz mitgeteilt, daß aufgrund der von mir geäußerten Bedenken künftig wie folgt verfahren werde:

1. Die meisten Behörden wollen dem Vorbild einer Staatsanwaltschaft folgen, die die Schreiben an die Leistungsempfänger dadurch anonymisiert, daß lediglich die Initialen des oder der Beschuldigten, Postleitzahl und Wohnort sowie das Aktenzeichen der Staatsanwaltschaft weitergegeben werden.
2. Bei einigen Staatsanwaltschaften werden Geldauflagen praktisch nur noch der Staatskasse zugewiesen.
3. Bei einigen Staatsanwaltschaften wird von einer Mitteilung an die gemeinnützige Einrichtung abgesehen; der durch Rückfragen ausgelöste Mehraufwand wird in Kauf genommen.

Aus meiner Sicht bestehen gegen keine der drei vorgeschlagenen Verfahrensweisen durchgreifende datenschutzrechtliche Bedenken: Bei den Varianten 2. und 3. werden keinerlei personenbezogene Mitteilungen an Stellen außerhalb der Justiz vorgenommen. Variante 1. sieht zwar eine Mitteilung an die Leistungsempfänger vor, allerdings erst nach teilweiser Anonymisierung. Den datenschutzrechtlichen Interessen des Betroffenen wird dadurch weitgehend Rechnung getragen.

7.3.4 Auskunft aus staatsanwaltschaftlichen Akten

.Im Berichtszeitraum erreichten mich mehrere Eingaben, die sich auf die Behandlung von Auskunftsbegehren durch die Staatsanwaltschaften bezogen.

In einem Fall wurde das Auskunftsbegehren des Petenten diesem mit der Bemerkung im Original zurückgesandt, eine Beantwortung seines Schreibens sei nicht veranlaßt. In einem anderen Fall weigerte sich die Behörde, dem Petenten Auskunft über die über ihn gespeicherten Verfahren in der zentralen Namensdatei zu geben.

Ich nehme dies zum Anlaß, darauf hinzuweisen, daß sich die Auskunftserteilung an Betroffene außerhalb eines konkreten Strafverfahrens mangels einer bereichsspezifischen gesetzlichen Regelung nach [Art. 10](#) des Bayerischen Datenschutzgesetzes richtet. Danach ist jede speichernde Stelle grundsätzlich verpflichtet, dem Betroffenen auf Antrag Auskunft zu erteilen über

- die zu seiner Person gespeicherten Daten,
- den Zweck der Speicherung sowie
- die Herkunft der Daten und deren Empfänger, soweit diese Angaben gespeichert sind.

Das bedeutet, daß dem anfragenden Bürger auf die Frage, welche Verfahren gegen ihn anhängig sind oder waren, die entsprechenden Daten mitgeteilt werden müssen.

Einschränkungen ergeben sich, wenn die jeweiligen personenbezogenen Daten, auf die sich die Auskunft bezieht, nicht in automatisierten Dateien gespeichert sind. Die Auskunft wird dann nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, wenn der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von dem Betroffenen geltend gemachten Informationsinteresse steht.

Die Auskunftserteilung unterbleibt, soweit gesetzliche Versagungsgründe vorliegen.

Lehnt eine Staatsanwaltschaft die Auskunftserteilung ab, so muß sie nach [Art. 10 Abs. 6 Satz 1 BayDSG](#) diese Ablehnung nicht begründen. Der Betroffene ist jedoch darauf hinzuweisen, daß er sich in diesem Fall an den Landesbeauftragten für den Datenschutz wenden kann. Ich werde dann die Rechtmäßigkeit der Auskunftsverweigerung und ggf. die Zulässigkeit der Speicherung überprüfen.

Das Staatsministerium hat die Thematik auf die Tagesordnung der nächsten Dienstbesprechung

mit den Leiterinnen und Leitern der bayerischen Staatsanwaltschaften gesetzt.

7.4 Gerichtlicher Bereich

7.4.1 Prüfungskompetenz

Bereits in meinem 16. Tätigkeitsbericht ([Nrn. 1.7](#) und [7.3.1](#)) habe ich zu Einschränkungen meiner Kontrollmöglichkeit im Bereich des Strafverfahrens Stellung genommen. Auch im laufenden Berichtszeitraum ist die Frage meiner Kontrollkompetenz bei Gerichten wieder aufgetreten:

[Art. 2 Abs. 6](#) Bayerisches Datenschutzgesetz nimmt Gerichte von meiner Kontrollkompetenz aus, es sei denn, sie werden "in Verwaltungsangelegenheiten" tätig. Aufgrund dieser Formulierung wird bisweilen die Auffassung vertreten, selbst Hilfstätigkeiten, die die Durchführung von Rechtspflegeaufgaben ermöglichen sollen, wie z.B. das Versenden gerichtlicher Schreiben durch die Geschäftsstellen, seien meiner Kontrollbefugnis entzogen. Diese Auffassung halte ich für unzutreffend. Sie widerspricht dem Sinn der gesetzlichen Regelung, die lediglich den grundgesetzlich geschützten Bereich der richterlichen Unabhängigkeit von meinen Kontrollen ausnehmen soll. Kontrollfreie Räume im öffentlichen Bereich sind im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zur Bedeutung der Datenschutzkontrolle eng zu halten und im gerichtlichen Bereich nur da gerechtfertigt, wo der Bereich der richterlichen Unabhängigkeit betroffen ist. Alle Tätigkeiten eines Gerichts, die der Verwirklichung unmittelbaren Rechtsschutzes im Einzelfall dienen und die in richterlicher Unabhängigkeit vorgenommen werden, unterliegen damit nicht meiner Prüfkompetenz. Dies ist im Hinblick auf den Grundsatz der Gewaltenteilung unbestritten. Hilfstätigkeiten und die Ordnungsmäßigkeit und Rechtmäßigkeit automatisierter Gerichtsverfahren und alle Aufgaben von Angehörigen eines Gerichts, die der Dienstaufsicht unterliegen und daher nicht in richterlicher Unabhängigkeit vollzogen werden, sollten meiner Kontrollkompetenz unterliegen.

Anlässlich der anstehenden Novellierung des Bayerischen Datenschutzgesetzes werde ich mich für eine klarstellende Regelung einsetzen, die einen zureichenden Kontrollumfang auch bei Gerichten sicherstellt. Angemessen wäre eine Formulierung, wie sie bereits in Schleswig-Holstein gilt:

"Die Gerichte unterliegen der Kontrolle der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz, soweit sie nicht in richterlicher Unabhängigkeit tätig werden."

Wir Datenschutzbeauftragten des Bundes und der Länder haben diese Forderung aufgegriffen und eine EntschlieÙung zur "Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten" gefaÙt ([Anlage 19](#)).

7.4.2 Entscheidungssammlungen bei den Gerichten

Aufgrund des Vorhabens des Bayerischen Verwaltungsgerichtshofs, Entscheidungen innerhalb der bayerischen Verwaltungsgerichtsbarkeit in automatisierter Form zugänglich zu machen, bin ich mit der Problematik der Führung von Entscheidungssammlungen bei Gerichten befaÙt worden.

Geplant war ein vertikaler Austausch von Entscheidungen zwischen dem Verwaltungsgerichtshof und den sechs bayerischen Verwaltungsgerichten sowie zwischen den Verwaltungsgerichten untereinander (horizontaler Austausch). Die Entscheidungen sollten zunächst auf CD-Rom, später im Behördennetz im Volltext übertragen werden und zwar in nichtanonymisierter Form.

Im Rahmen meiner Beratungstätigkeit gegenüber dem Verwaltungsgerichtshof habe ich grundsätzlich ein berechtigtes Interesse an einem Entscheidungsaustausch der beteiligten Stellen anerkannt. Ein solcher dient einer möglichst weitgehenden Einheitlichkeit der Rechtsprechung und damit letztlich auch der Rechtsklarheit.

Ich habe jedoch deutlich gemacht, daß ich die Einstellung nichtanonymer Entscheidungen zum Zwecke des Abrufs durch andere Gerichte aus datenschutzrechtlicher Sicht für nicht erforderlich halte, weil der Zweck der Entscheidungssammlung auch durch **anonymisierte Entscheidungen** erreicht werden kann.

Ich habe auch deutlich gemacht, daß der mit einer Anonymisierung verbundene Aufwand auch angesichts der Vielzahl von 25.000 Altentscheidungen als eher gering einzuschätzen ist. Die Namen von ProzeÙbeteiligten, Sachverständigen und Zeugen lassen sich ohne weiteres mit einer Suchroutine finden und ersetzen.

Der Präsident des Bayerischen Verwaltungsgerichtshofes hat meine Bedenken berücksichtigt und meinen Anregungen Rechnung getragen. Hinsichtlich neu einzustellender Entscheidungen wurden die Richter gebeten, Texte möglichst neutral zu halten und dann, wenn dies nicht möglich sei, bereits beim Diktieren personenbezogene Daten besonders zu markieren.

Bezüglich der Altentscheidungen werden das Rubrum gelöscht und, soweit möglich, personenbezogene Daten auch im Text anonymisiert. Die Einhaltung dieser Vorgaben wird durch die Gerichtsverwaltung bei Alt- und bei Neufällen stichprobenartig kontrolliert werden.

Bei einem ähnlichen Projekt im Bereich der Finanzgerichtsbarkeit hält das Finanzministerium die Speicherung personenbezogener Daten zur Wahrung der Einheitlichkeit der Rechtsprechung in Verfahrensfragen sowie im materiellen Recht für zulässig. Ich habe deutlich gemacht, daß dies nicht der Fall ist, da für die Einheitlichkeit der Rechtsprechung die Namen der Beteiligten ohne Belang sind. Ich habe darauf hingewiesen, daß es zahlreiche Entscheidungssammlungen gibt, die ohne Nennung personenbezogener Daten auskommen. Ferner habe ich auf die Handhabung am Bayerischen Verwaltungsgerichtshof hingewiesen. Ich habe deutlich gemacht, daß ich nur mit der Errichtung einer Entscheidungssammlung in anonymisierter Form einverstanden bin.

Das Staatsministerium der Finanzen hat inzwischen eine Prüfung eingeleitet, ob eine Entscheidungssammlung auch im dortigen Bereich in anonymisierter Form durchgeführt wird. Ein Ergebnis steht noch aus.

7.4.3 Aussonderung von Spruchkammerakten

Durch eine schriftliche Anfrage von Abgeordneten des Bayerischen Landtags bin ich darauf aufmerksam geworden, daß Spruchkammerakten noch immer bei den Amtsgerichten aufbewahrt werden, in deren Bezirk die Spruchkammern ihren Sitz hatten. Sie sind bislang den Staatsarchiven nicht zur Übernahme angeboten worden. Das Staatsministerium der Justiz hat hierzu mitgeteilt, daß Einvernehmen zwischen Justiz- und Kultusministerium bestünde, die Spruchkammerakten vorerst weiterhin bei den Amtsgerichten aufzubewahren und zunächst noch keinen konkreten Termin für die Aussonderung festzulegen. Im Hinblick darauf, daß nach wie vor Anträge auf Erteilung von Auskünften und auf Akteneinsicht gestellt würden, sei eine Entscheidung über diese Frage zunächst bis zum Jahr 2000 vorbehalten worden.

Auf meine Nachfrage hat das Staatsministerium der Justiz ergänzt, daß nach dort vorliegenden Berichten der Praxis nicht bekannt sei, daß die Spruchkammerakten auch noch zu anderen Zwecken herangezogen würden als zur Klärung von Rechtsansprüchen Betroffener oder Hinterbliebener, zur wissenschaftlichen Forschung, zu Rentenangelegenheiten, Israelreisen, Ehrung

von Bürgern sowie zur Erfüllung von Aktenanforderungen oberster Dienstbehörden, Gerichten und Staatsanwaltschaften. Nach dem Ergebnis einer repräsentativen Umfrage würden die Spruchkammerakten getrennt von sonstigen Akten aufbewahrt. Zugriff auf diese Unterlagen könnten nur diejenigen Personen nehmen, die auch dienstlich mit der Entscheidung über Anträge auf Erteilung von Auskünften aus Akten und Registern der Spruchkammerakten sowie auf Einsicht in diese Akten befaßt seien, also der Präsident bzw. Direktor des Amtsgerichts, der Geschäftsleiter, der Sachbearbeiter oder der Registrator.

Daraufhin habe ich mich nochmals an das Staatsministerium der Justiz gewandt und dargelegt, daß ich seinem Schreiben entnehme, daß die Spruchkammerakten zur Erfüllung der Aufgaben **der Justiz** nicht mehr benötigt werden. Ich habe deutlich gemacht, daß sie daher grundsätzlich gemäß Art. 6 Abs. 1 Satz 1 Bayerisches Archivgesetz dem zuständigen staatlichen Archiv zur Übernahme anzubieten sind.

Inzwischen ist das Justizministerium an das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst herantreten und hat signalisiert, daß seitens des Staatsministeriums der Justiz keine Bedenken gegen eine Abgabe dieser Akten an die Archive bestünden.

Eine Äußerung des Kultusministeriums steht noch aus.

7.4.4 Übermittlung von Daten aus dem Schuldnerverzeichnis auf Datenträger in maschinell lesbarer Form

§ 915 d Abs. 1 Satz 1 ZPO sieht vor, daß auf Antrag Abdrucke aus dem Schuldnerverzeichnis zum laufenden Bezug auch in einer nur maschinell lesbaren Form übermittelt werden können. Auf meine Anfrage an das Staatsministerium der Justiz, ob und in welchem Umfang von dieser Möglichkeit Gebrauch gemacht wird, wurde mir geantwortet, daß dies bislang lediglich bei drei Amtsgerichten der Fall sei. Lediglich eine Firma erhalte derzeit Abdrucke in dieser Form.

Das Staatsministerium der Justiz hat weiter mitgeteilt, daß für die Übermittlung von Daten aus dem Schuldnerverzeichnis in einer nur maschinell lesbaren Form keine Ablaufregelungen erlassen worden seien. Die ist nach § 915 d Abs. 1 Satz 2 ZPO aber vorgeschrieben. Darauf habe ich das Ministerium hingewiesen. Die folgenden Ablaufregelungen halte ich für zweckmäßig:

- Nachvollziehbare Dokumentation der Datenübermittlungen,

- Virenprüfung von Fremddisketten durch ein Anti-Viren-Schutzprogramm,
- Versand der Datenträger in verschlossenem Umschlag mit Zustellungsurkunde oder als Einschreiben mit Rückschein oder alternativ Verschlüsselung der Daten auf den Datenträgern, sowie
- verbindliche Vorgaben über die Datenlöschung und die Rückgabe nicht mehr benötigter Datenträger durch den Empfänger.

Nach Auskunft des Staatsministeriums der Justiz hat eine Umfrage bei den Justizministerien der Länder ergeben, daß bisher von keiner Landesjustizverwaltung entsprechende Ablaufregelungen für die Übermittlung von Abdrucken in einer maschinell lesbaren Form aus dem Schuldnerverzeichnis erlassen wurden. Es sei jedoch zwischenzeitlich eine Arbeitsgruppe eingesetzt worden, die bis zur nächsten Sitzung der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz einen Regelungsentwurf hierfür vorlegen soll.

Das Staatsministerium der Justiz wird vor dem Entwurf eigener Ablaufregelungen zunächst die Ergebnisse dieser Arbeitsgruppe abwarten um sich an einem bundesweiten Musterentwurf orientieren zu können.

Dies halte ich grundsätzlich für sachgerecht und zweckmäßig. Allerdings wäre es notwendig gewesen, Ablaufregelungen bereits vor einer Übermittlung von Daten in maschinell lesbarer Form zu erlassen.

Zwischenzeitlich liegt ein Entwurf der Arbeitsgruppe vor, bei dessen Erarbeitung der saarländische Landesbeauftragte für den Datenschutz beteiligt war. Die vorgesehenen Datenübertragungsregelungen beschränken sich auf die Datenübertragung im Wege des Datenträgertausches und erfüllen meine Vorgaben.

7.4.5 Zusammenarbeit der Justizbehörden mit den Medien - Entwurf einer Presserichtlinie

Bereits in meinem 17. Tätigkeitsbericht ([Nrn. 7.6.2](#) und [7.6.3](#)) habe ich über den Stand der Diskussion mit dem Justizministerium über die Weitergabe personenbezogener Daten durch die Strafverfolgungsbehörden an die Medien berichtet. Ich habe dargestellt, daß ich eine solche Übermittlung nur **ausnahmsweise** für gerechtfertigt halte, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

Das Staatsministerium der Justiz hat mir inzwischen den Entwurf einer Neufassung der Presserichtlinien übersandt. Der Entwurf entspricht in weiten Teilen schon jetzt den Belangen des Datenschutzes. Allerdings sollte nach meiner Auffassung noch stärker zum Ausdruck gebracht werden, daß der Informationsanspruch der Presse in jedem Fall einer Abwägung mit den Grundrechten Betroffener bedarf. Eine aktive Öffentlichkeitsarbeit der Justizbehörden sollte - soweit sie personenbezogen erfolgt - grundsätzlich unterbleiben. Unter diesen Gesichtspunkten habe ich eine Reihe konkreter Vorschläge gemacht, von denen mir die nachfolgenden besonders wichtig erscheinen:

Der Entwurf sieht vor, daß den Gerichtsberichterstatern in Schwurgerichtssachen und in Strafsachen, von denen anzunehmen ist, daß sie in der Öffentlichkeit besondere Beachtung finden werden und die für die Öffentlichkeit von überwiegendem Interesse sind, vor der Hauptverhandlung eine Abschrift des Anklagesatzes überlassen werden darf. Bei der Entscheidung, ob ein Anklagesatz herausgegeben wird, sind insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten und deren Angehörige, die Schwere, die Umstände und die Folgen der Tat zu beachten. Die Überlassung des Anklagesatzes ist erst nach Eröffnung des Hauptverfahrens statthaft. Ich habe darauf hingewiesen, daß ich es für nicht erforderlich halte, Pressevertretern bereits erhebliche Zeit vor einer Hauptverhandlung den Anklagesatz zur Verfügung zu stellen und habe deshalb vorgeschlagen, in der Richtlinie vorzuschreiben, daß Abschriften des Anklagesatzes frühestens eine Woche vor der Hauptverhandlung herausgegeben werden dürfen. Der Entwurf sieht ferner vor, daß spätestens am Ende einer Woche die **Sitzungslisten** der Strafverhandlungen, die in der folgenden Woche am Sitzungsort stattfinden, zur Einsichtnahme durch

die Gerichtsberichterstatter ausgelegt werden. In der Regel seien die Nachnamen der Angeklagten bis auf den jeweiligen Anfangsbuchstaben unkenntlich zu machen.

Ich habe diese Formulierung für mißverständlich gehalten, weil sie den Eindruck erweckt, sie bezwecke die Festlegung eines Zeitpunktes, an welchem die Auslegung spätestens beginnen muß. Tatsächlich ist aber entscheidend, daß die Listen frühestens dann ausgelegt werden dürfen, wenn eine zeitliche Nähe zum Hauptverhandlungstermin besteht. Ich habe daher vorgeschlagen, die Worte "spätestens am Ende einer Woche" durch die Worte "in der Vorwoche" zu ersetzen. Darüber hinaus habe ich gefordert, die Worte "in der Regel" zu streichen, da kein Grund ersichtlich ist, Ausnahmen von der Teilanonymisierungspflicht zuzulassen.

Eine Antwort des Staatsministeriums der Justiz auf meine Vorschläge steht noch aus.

7.5 Justizvollzugsanstalten

7.5.1 Zugriff auf Gefangenpersonalakten

Bereits in meinem 16. Tätigkeitsbericht ([Nr. 7.3.3.1](#)) sowie in meinem 17. Tätigkeitsbericht ([Nr. 7.3.2.1](#)) habe ich mich mit der Frage des Zugriffs auf Gefangenpersonalakten befaßt. Ich habe dabei stets gefordert, daß der Zugriff auf Gefangenpersonalakten nur in dem Umfang gewährt werden soll, wie er zur Erfüllung der Aufgaben des jeweiligen Vollzugsbediensteten erforderlich ist. In den meisten Justizvollzugsanstalten hat derzeit faktisch jeder Vollzugsbedienstete Zugriff auf alle Gefangenpersonalakten. Das gilt auch für besonders sensible Daten wie z.B. angehaltene Briefe an den Gefangenen oder Unterlagen über eine Besucherüberprüfung. Ferner habe ich im Interesse einer späteren Nachvollziehbarkeit gefordert, daß sowohl die Entnahme als auch die Einsichtnahme in Gefangenpersonalakten auf der Geschäftsstelle unter Angabe von Datum, Handzeichen bzw. Unterschrift und Entnahme- bzw. Einsichtsgrund zu dokumentieren ist.

Bei der Prüfung einer Justizvollzugsanstalt habe ich eine Praxis festgestellt, die meinen Vorstellungen näher kommt als dies in den meisten anderen Justizvollzugsanstalten der Fall ist: Die Aktenentnahme ist dort nur dem Anstaltsleiter, seinem Stellvertreter, den Sozialpädagogen (drei) und dem Psychologen sowie den Sachbearbeitern in Gnaden- und Vollstreckungsverfahren gestattet. Alle anderen Personen erhalten nur auf der Vollzugsgeschäftsstelle Einsicht in die Gefangenpersonalakte. Die Entnahme wird stets, die Einsichtnahme häufig dokumentiert, wobei

allerdings der Grund der Einsichtnahme nicht angegeben wird. Festgehalten werden lediglich der Zeitpunkt der Entnahme und der Zeitpunkt der Rückgabe mit dem jeweiligen Handzeichen des Bediensteten.

Diese Handhabung weist in die richtige Richtung. Aus datenschutzrechtlicher Sicht sollte jedoch eine **vollständige Protokollierung aller Einsichtnahmen und die Dokumentation des Einsichtsgrundes erfolgen**. Zwar mag die Dokumentation des Einsichtsgrundes Mißbrauch nicht in allen Fällen verhindern, die präventive Wirkung einer solchen Maßnahme sollte aber nicht unterschätzt werden.

Meinem Vorschlag, auch den Einsichts- bzw. Entnahmegrund zu dokumentieren ist die Justizvollzugsanstalt nicht nähergetreten. Im Vergleich mit der zu erzielenden präventiven Wirkung gegen evtl. denkbare Mißbrauchsfälle stünde der erhebliche zusätzliche Verwaltungsaufwand außer Verhältnis.

Auch der Beirat beim Landesbeauftragten für den Datenschutz hat sich erneut mit der Thematik befaßt. Auf ein **Schreiben des Beiratsvorsitzenden**, mit dem er eine differenzierte Zugriffsbefugnis befürwortet, hat der Staatsminister der Justiz ablehnend reagiert. Der Zugriff auf die Daten des Gefangenen dürfe nur dort beschränkt werden, wo höherrangige Interessen dies gebieten. Das sei zwar bei den Gesundheitsakten der Fall, weil hier ein besonderes Vertrauensverhältnis zwischen dem Anstaltsarzt und dem Gefangenen zu schützen ist, bei den übrigen Gefangenenpersonalakten könne sich der Gefangene indes nicht auf vergleichbare hochrangige Geheimhaltungsinteressen berufen. Der Staatsminister der Justiz hat ferner darauf hingewiesen, daß es keinerlei Anhaltspunkte für eine mißbräuchliche Verwendung von Daten Gefangener durch bayerische Justizvollzugsbedienstete gebe. Hinsichtlich der Dokumentation von Zugriffen auf die Gefangenenpersonalakte wurde darauf verwiesen, daß eine solche Pflicht auch durch das Vierte Strafvollzugsänderungsgesetz nicht eingeführt werde. Eine Änderung der Verwaltungspraxis in den bayerischen Justizvollzugsanstalten werde daher nicht veranlaßt.

Ich bedaure diese starre Haltung sehr, weil damit ein unbeschränkter Zugriff aller Bediensteter auf sämtliche Daten nach wie vor möglich ist und etwaige Mißbräuche mangels Dokumentation nach Einsichtnahme nicht festgestellt werden können. Weshalb zwischen Arzt und Patient ein größeres Vertrauensverhältnis bestehen soll als etwa zwischen Proband und Sozial- oder Psychotherapeut, vermag ich nicht nachzuvollziehen. Die Haltung des Justizministeriums verwundert um so mehr, als derartige Forderungen in anderen deutschen Ländern ohne weiteres umge-

setzt werden. Z.B. hat die Thüringer Landesregierung in ihrer Stellungnahme zum 2.Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz zu Nr. 10.17 ausgeführt, daß die Einsichtnahme in Gefangenenpersonalakten funktionsbezogen geregelt werden könne. Die Kontrolle des beschränkten Einsichtsnahmerechts und die Dokumentation der Einsichtnahme sei den Leitern der Vollzugsgeschäftsstellen in den Justizvollzugsanstalten übertragen worden. Unterlagen über psychologische, psychiatrische, psychotherapeutische und sozialtherapeutische Behandlungen sowie Unterlagen über andere besonders sensible Gefangenen-daten würden getrennt von anderen Personalunterlagen der Gefangenen geführt und nur einem sehr beschränkten Kreis von Vollzugsbediensteten zugänglich gemacht.

7.5.2 Verteilung des "A-Bogens"

In meinem letzten Tätigkeitsbericht ([Nr. 7.3.2.4](#)) habe ich mich mit der Frage der Übermittlung der Daten des Personalblatts des Gefangenen (A-Bogen) befaßt. Ich halte an meiner dort geäußerten Auffassung fest, daß die zahlreichen Daten des A-Bogens nur in dem Umfang an die einzelnen Stellen der Anstalt übermittelt werden dürfen, in dem sie für die Aufgabenerfüllung des jeweiligen Empfängers tatsächlich benötigt werden.

Über die Handhabung der Verteilung des A-Bogens habe ich mich erneut bei der Prüfung einer Justizvollzugsanstalt unterrichtet.

Dabei hat sich ergeben, daß der vollständige Datensatz des A-Bogens undifferenziert an eine Vielzahl von Stellen innerhalb der Anstalt weitergegeben wird. Ich habe darauf hingewiesen, daß mir diese Praxis problematisch erscheint und daß spätestens mit Einführung der EDV in den Vollzugsgeschäftsstellen im Detail geklärt sein sollte, welche Stelle welche Daten für die Erfüllung der ihr zugewiesenen Aufgaben sowie zur Zusammenarbeit innerhalb der Justizvollzugsanstalt benötigt. Nur diese Daten sollten übermittelt werden.

Die Anstalt hat daraufhin mitgeteilt, daß sie aufgrund meiner Hinweise die Überlassung des A-Bogens an Seelsorger, Psychologen und Sozialpädagogen eingestellt hat.

Im Rahmen der Automation der Aufgaben der Vollzugsgeschäftsstelle und der Einrichtung eines Informationssystems über Gefangenen-daten (siehe dazu [Nr. 7.2.4](#)) sollten datenschutzgerechte Lösungen in allen bayerischen Vollzugsanstalten möglich sein. Ich habe das Staatsministerium der Justiz darauf hingewiesen, daß nach meiner Einschätzung mit Hilfe der EDV die Erstellung

differenzierter A-Bögen mit vertretbarem Aufwand möglich sein dürfte. Das Ministerium hat zugesagt, bei der Entwicklung eines entsprechenden Informationskonzeptes auch die differenzierte Weitergabe von Daten des A-Bogens an Bedienstete, die nicht über Bildschirmarbeitsplätze verfügen, in die Prüfung einzubeziehen.

7.5.3 Telefongespräche Gefangener

In einer Justizvollzugsanstalt habe ich die Praxis der Überwachung von Telefongesprächen Gefangener durch Anstaltsbedienstete überprüft. Dort können nicht nur Untersuchungsgefangene mit richterlicher Genehmigung, sondern auch Strafgefangene in dringenden und wichtigen Fällen (z.B. in Krankheitsfällen oder bei besonderen persönlichen Problemen) Telefongespräche führen. Die Entscheidung, ob ein Telefonat geführt werden darf, trifft der jeweils zuständige Sozialarbeiter, der in seinem Dienstzimmer das Telefonat vermittelt. Das bedeutet, daß der Sozialarbeiter selbst wählt und dem vom Gefangenen gewünschten Gesprächspartner das Gespräch ankündigt. Dabei wird er durch den Sozialarbeiter auch über das beabsichtigte Mithören informiert. Im Regelfall werden alle Gespräche mitgehört, wohl jedoch nicht Gespräche mit Rechtsanwälten und nach Entscheidung im Einzelfall.

Ich habe begrüßt, daß die Angerufenen vor einem Gespräch jeweils über das beabsichtigte Mithören in Kenntnis gesetzt werden. Allerdings mußte ich feststellen, daß keine Sicherheit darüber zu bestehen scheint, in welchen Fällen vom Mithören abzusehen ist. Ich habe mich daher an das Staatsministerium der Justiz gewandt und angeregt, u.a. festzulegen,

- welche Telefonate überwacht werden dürfen und
- in welcher Form die Überwachung durchzuführen ist (z.B. Mithören nach vorheriger Vermittlung des Gesprächs und Information des Gesprächspartners).

In diesem Zusammenhang habe ich auch darauf hingewiesen, daß **Gespräche mit Verteidigern** nach dem Strafvollzugsgesetz nicht mitgehört werden dürfen.

Das Staatsministerium der Justiz hat die Problematik auf einer Dienstbesprechung mit den Leitern der bayerischen Justizvollzugsanstalten erörtert und mitgeteilt, daß aus dortiger Sicht eine generelle Regelung nicht erforderlich erscheint. Es bestünden jedoch "keine grundsätzlichen Bedenken" dagegen, den Gefangenen im voraus und den Angerufenen zu Beginn des Telefonge-

sprächs von der Tatsache der Überwachung zu unterrichten. Meine Auffassung, daß Gespräche mit Verteidigern nicht überwacht werden dürfen, vermag das Staatsministerium der Justiz nicht zu teilen. Es bestehe keine Möglichkeit, festzustellen, ob der Gesprächspartner des Gefangenen tatsächlich sein Verteidiger ist. Ein Mißbrauch könne nur durch Überwachung des Telefongesprächs ausgeschlossen werden.

In der Zwischenzeit ist durch Änderung des Strafvollzugsgesetzes bei einer Überwachung fernmündlicher Gespräche die beabsichtigte Überwachung dem Gesprächspartner des Gefangenen unmittelbar nach Herstellung der Verbindung durch die Vollzugsbehörde oder den Gefangenen mitzuteilen. Der Gefangene ist rechtzeitig vor Beginn der fernmündlichen Unterhaltung über die beabsichtigte Überwachung und die Mitteilungspflicht zu unterrichten.

Unverständlich ist, daß meine Auffassung hinsichtlich des Überwachungsverbotes von Telefongesprächen mit Verteidigern nicht geteilt wird, obwohl sich dieses Verbot unmittelbar aus dem Gesetz selbst ergibt. Angesichts der eindeutigen Rechtslage ist der Hinweis auf Schwierigkeiten in der Praxis, die Verteidigereigenschaft fernmündlich festzustellen, ohne Bedeutung. Ich habe deutlich gemacht, daß die Anstalt jederzeit die Möglichkeit hat, im Einzelfall die Durchführung eines Telefongesprächs entweder abzulehnen oder mit Einverständnis des Gefangenen und des Verteidigers ein überwachtes Gespräch zuzulassen, wenn Zweifel an der Verteidigereigenschaft des Telefonpartners bestehen. Sollte ich die unzulässige Überwachung eines Verteidigergesprächs feststellen, werde ich das beanstanden.

Das Justizministerium wird die Frage erneut auf einer Dienstbesprechung mit den Leiterinnen und Leitern der Justizvollzugsanstalten erörtern.

7.6 Ordnungswidrigkeitenverfahren

7.6.1 Überwachung des ruhenden und des fließenden Verkehrs durch Gemeinden

In meinem 17. Tätigkeitsbericht ([Nr. 7.5.2.1](#)) habe ich davon berichtet, daß aufgrund einer Änderung der Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht seit 01.10.1994 zahlreiche Städte und Gemeinden in Bayern die Befugnis erhalten haben, selbst Geschwindigkeitskontrollen durchzuführen und entsprechende Verstöße zu verfolgen. Die Zahl derjenigen Städte und Gemeinden mit eigenen Kompetenzen im Ordnungswidrigkeitenverfahren ist seither noch gestiegen. Seit 01.11.1997 haben 254 Städte und Gemeinden die Befugnis, Parkverstöße mit

eigenen Außendienstkräften zu verfolgen und Parksünder zu verwarnen, 103 Städte und Gemeinden dürfen Tempoverstöße verfolgen, 83 dürfen zu diesem Zweck auch Bußgeldbescheide erlassen. Mit der verstärkten Einbeziehung von Kommunen in die Verkehrsüberwachung will das Staatsministerium des Innern die Verkehrssicherheit durch zusätzliche Kontrollen erhöhen und zugleich die Polizei entlasten.

Erstmals in diesem Berichtszeitraum habe ich datenschutzrechtliche Kontrollen der kommunalen Verkehrsüberwachung in zwei kreisfreien Städten durchgeführt. Dabei habe ich eine Reihe von Mängeln festgestellt.

Das Staatsministerium des Innern hat es begrüßt, daß ich derartige Überprüfungen vornehme. Es hat darauf hingewiesen, daß sich das Verfahren bei der kommunalen Geschwindigkeitsüberwachung, das es in Bayern erst seit 1994 gibt, und das durch verschiedene Gerichtsentscheidungen beeinflußt und modifiziert wurde, trotz entsprechender Vorgaben des Staatsministeriums des Innern noch nicht ganz vereinheitlicht und gefestigt habe.

Neben der Behandlung von Fragen der Übertragung hoheitlicher Tätigkeiten auf Private (s. unten [Nr.7.6.2](#)), der Speicherung von Mehrfachtätern (s. unten [Nr. 7.6.3](#)) und der Nutzung des Paß- bzw. Personalausweisregisters zur Identifizierung von Verkehrssündern (s. unten [Nr. 7.6.4](#)) habe ich auf folgendes hingewiesen:

1. Alle automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedürfen grundsätzlich der **vorherigen schriftlichen Freigabe** durch die öffentliche Stelle, die nach [Art. 25 BayDSG](#) für den Datenschutz verantwortlich ist. Das ist bei Verfahren, die im Bereich der kommunalen Verkehrsüberwachung eingesetzt werden, die jeweilige Gemeinde.
2. Die Speicherdauer von Verfahren sollte einen Zeitraum von vier Monaten nach Abschluß des Verfahrens grundsätzlich nicht überschreiten. Nach diesem Zeitpunkt sind allen Daten, die nicht dem Auffinden der Akten dienen, zu löschen oder -falls dies nicht möglich ist - zu sperren.
3. Die Akten der kommunalen Verkehrsüberwachung sollten getrennt von anderen Akten in verschließbaren Schränken aufbewahrt werden. Sie sollten nicht länger aufbewahrt werden, als dies bei der Polizei vorgesehen ist. Sofern Bußgeldverfahren von der Zentralen Bußgeldstelle bearbeitet werden, sollte diese den Verfahrensausgang mitteilen. Sofern binnen angemessener Zeit keine Rückmeldung über den Ausgang des Verfahrens erfolgt,

sollte regelmäßig angefragt werden.

4. Daten in einem "Erfassungs-PC" sollten dort allenfalls kurze Zeit gespeichert bleiben, nachdem sie auf das Sachbearbeitungssystem übertragen worden sind.

7.6.2 Verlagerung von Aufgaben der kommunalen Verkehrsüberwachung auf Private

In meinem 17. Tätigkeitsbericht ([Nr. 7.5.2](#) ff.) habe ich mich zu der Problematik der Beteiligung Privater bei der Erfüllung hoheitlicher Aufgaben im Bereich der Parkraumüberwachung und im Bereich der Überwachung des fließenden Verkehrs geäußert.

Die Überlegungen, bis zu einer grundsätzlichen Klärung durch die Rechtsprechung häufige Stichproben anstelle einer ständigen Überwachung der Bediensteten, die mit einem Meßvorgang betraut sind, für ausreichend anzusehen, sind inzwischen durch zwei Entscheidungen des Bayerischen Obersten Landesgerichts gegenstandslos geworden.

7.6.2.1 Entscheidung des Bayerischen Obersten Landesgerichts vom 05.03.1997

Das Bayerische Oberste Landesgericht hat am 05.03.1997 entschieden, daß mangels gesetzlicher Ermächtigung eine Gemeinde, die für die Verfolgung von Ordnungswidrigkeiten (**Geschwindigkeitsüberwachung**) zuständig ist, nicht befugt ist, eine private Firma mit der Messung, Registrierung und Dokumentation von Geschwindigkeitsverstößen zu beauftragen, auch wenn die Gemeinde Ort, Zeit und Dauer der Messung bestimmt und die Auswertung der Meßergebnisse selbst vorgenommen hat.

Maßnahmen der Geschwindigkeitsüberwachung bei der Ermittlung und Verfolgung der sich daraus ergebenden Verkehrsverstöße seien hoheitlicher Natur und in der Regel Angehörigen des öffentlichen Dienstes vorbehalten. Auf dem Gebiet der öffentlichen Sicherheit könne eine Privatisierung in aller Regel **nur in der Gestalt der Beleihung Privater** erfolgen, die einer gesetzlichen Ermächtigung bedürfe.

Eine funktionale Privatisierung in der Form einer bloßen Verwaltungshilfe scheidet ebenfalls aus. Die planmäßige Ermittlung und Dokumentation von Geschwindigkeitsverstößen stehe in einem unmittelbaren Zusammenhang mit der originären Staatsaufgabe der Verfolgung und Ahndung

von Ordnungswidrigkeiten. Die hoheitliche Sanktion baue direkt auf dem Ermittlungsergebnis auf, weshalb die Ermittlung, Dokumentation, Verfolgung und Ahndung des jeweiligen Verkehrsverstoßes rechtlich gesehen eine Einheit bildeten. Systematische Geschwindigkeitsmessungen durch beauftragte Privatunternehmer seien funktionell Staatsaufgaben und nicht rein technische Hilfsdienste.

Die Ahndung von Geschwindigkeitsverstößen durch Leiharbeitnehmer nach Maßgabe des Arbeitnehmerüberlassungsgesetzes (AÜG) sei jedenfalls dann nicht zulässig, wenn diese Leiharbeitnehmer nicht in die Gemeindeverwaltung physisch-räumlich und organisatorisch integriert seien.

Das Staatsministerium des Innern hat daraufhin seine Verwaltungsvorschriften angepaßt und vorgeschrieben, daß Geschwindigkeitsmessung (und die Entwicklung sowie Auswertung der Filme) künftig nur noch durch eigenes Personal der Stadt/Gemeinde zulässig oder aber durch privates Bedienpersonal unter **ständiger Aufsicht** eines entsprechend kundigen Bediensteten der Kommune durchgeführt werden dürfen. Daneben wird es grundsätzlich als zulässig angesehen, daß Kommunen sich von einem privaten Vertragspartner Personal nach Maßgabe des Arbeitnehmerüberlassungsgesetzes zur Verfügung stellen lassen. Allerdings dürfe der Einsatz von Leiharbeitnehmern nicht zu einer Umgehung des AÜG führen. Eine derartige Gestaltung dürfe daher nur als Übergangslösung gewählt werden. Die überlassenen Arbeitnehmer müßten sowohl organisatorisch als auch räumlich in die jeweilige Gemeinde integriert werden, der für das Verfahren zuständigen Organisationseinheit der Gemeinde zugeordnet und deren Leiter unterstellt werden.

Ich habe bei meinen Prüfungen ein besonderes Augenmerk auf die Einhaltung der genannten Kriterien gelegt. Dabei habe ich festgestellt, daß eine Stadt für die Überwachung des fließenden Verkehrs den bisher von einer privaten Stelle zur Verfügung gestellten Arbeitnehmer als nicht vollbeschäftigten Angestellten befristet eingestellt hat. Dieser Mitarbeiter hat eine förmliche Verpflichtungserklärung abgegeben. Bei Krankheit des Mitarbeiters stellt die private Firma geeignetes Personal zur Verfügung. In diesem Fall sitzt jeweils ein besonders geschulter Mitarbeiter der Stadt ständig neben dem Ersatzmann im Außendienstfahrzeug. Diese Gestaltung außerhalb des Arbeitnehmerüberlassungsgesetzes begegnet keinen Bedenken. Da der eingesetzte Mitarbeiter Angestellter der Gemeinde ist, darf er auch hoheitliche Aufgaben wahrnehmen. Im Krankheitsfall ist eine ständige Überwachung des externen Mitarbeiters gewährleistet.

Allerdings habe ich festgestellt, daß die Fotos nach Durchführung der Messung von einer privaten Firma entwickelt und erst dann an die Stadt übersandt werden. Zwar hat sich die Firma zur Einhaltung des Datengeheimnisses verpflichtet. Verpflichtungen einzelne Mitarbeiter nach dem Verpflichtungsgesetz lagen aber nicht vor. Zudem hat das Bayerische Staatsministerium des Innern infolge der Entscheidung des Bayerischen Obersten Landesgerichts ausdrücklich festgestellt, daß bei Geschwindigkeitsmessungen auch die Entwicklung und Auswertung der Filme nur durch eigenes Personal der Stadt/Gemeinde zulässig ist oder durch privates Personal unter ständiger Aufsicht eines entsprechend kundigen Bediensteten der Kommune.

Bei der zweiten von mir überprüften Gemeinde werden zur Überwachung des fließenden Verkehrs ausschließlich eigene Mitarbeiter eingesetzt. Allerdings sollte die Filmentwicklung nicht durch eine private Firma, mit der im Zeitpunkt meiner Prüfung noch nicht einmal eine schriftliche Vereinbarung geschlossen war, vorgenommen werden.

7.6.2.2 Entscheidung des Bayerischen Obersten Landesgerichts vom 11.07.1997

In seiner Entscheidung vom 11.07.1997 hat das Bayerische Oberste Landesgericht festgestellt, daß eine Gemeinde mangels gesetzlicher Ermächtigung nicht befugt ist, eine private Firma **mit der Überwachung des ruhenden Verkehrs** zu beauftragen, auch wenn die Gemeinde selbst die Auswertung der festgestellten Parkverstöße sowie den Erlaß der Bußgeldbescheide vornimmt. Es hätten die gleichen Erwägungen Geltung, die das Gericht bereits im Beschluß vom 05.03.1997 für Maßnahmen der Geschwindigkeitsüberwachung angestellt habe. Das Staatsministerium des Innern hatte für diesen Bereich bereits zuvor darauf hingewiesen, daß die Entscheidung des Bayerischen Obersten Landesgerichts zur Geschwindigkeitsüberwachung uneingeschränkt auch für die Überwachung des ruhenden Verkehrs Geltung habe.

Diese Auffassung habe ich geteilt und bei den von mir durchgeführten Prüfungen darauf geachtet, ob diese Vorgaben auch bei der Überwachung des ruhenden Verkehrs eingehalten werden. Hierbei habe ich festgestellt, daß in einer Gemeinde derzeit sechs Personen einer privaten Firma zur Überwachung des ruhenden Verkehrs eingesetzt werden. Deren Rechtsverhältnis richtet sich nach dem Arbeitnehmerüberlassungsgesetz. Die Firma verfügt über die notwendige Erlaubnis zur gewerbsmäßigen Arbeitnehmerüberlassung. Hinsichtlich jedes einzelnen Leiharbeitnehmers

ist ein Vertrag zur Arbeitnehmerüberlassung geschlossen worden. In einer Nebenabrede zu den Arbeitsverträgen erklären sich die überlassenen Arbeitnehmer ausdrücklich damit einverstanden, daß sie während des Einsatzes in der kommunalen Verkehrsüberwachung der Stadt gegenüber weisungsunterworfen sind. Vor ihrer Verwendung wird überprüft, ob sie für einen Einsatz im öffentlichen Dienst geeignet wären. Dies geschieht durch eine Erklärung zur Verfassungstreue sowie durch Anforderung eines Führungszeugnisses. Die Mitarbeiter geben zudem eine förmliche Verpflichtungserklärung ab. Die Firma bleibt Arbeitgeberin der überlassenen Personen, gewährt Urlaub und bezahlt sie. Bei Krankheit wird zunächst versucht, einen internen Ausgleich vorzunehmen. Ist dies nicht möglich, stellt die Firma geeignete Ersatzleute zur Verfügung. Die überlassenen Arbeitnehmer sind in Räumen untergebracht, die von der Stadt angemietet wurden. Da nach dem Arbeitnehmerüberlassungsgesetz der Einsatz eines Arbeitnehmers bei der gleichen Stelle nur für maximal zwölf Monate zulässig ist und ein erneuter Einsatz erst nach dreimonatiger Pause in Betracht kommt, werden derzeit verschiedene Lösungsmodelle erwogen.

Ich habe darauf hingewiesen, daß nach der Zielsetzung des Arbeitnehmerüberlassungsgesetzes durch den Einsatz eines Leiharbeitnehmers kein Dauerarbeitsplatz besetzt werden darf. Eine ständige Aneinanderreihung von Leiharbeitsverhältnissen ist daher - auch nach Einschätzung des Staatsministeriums des Innern - unzulässig.

Die andere von mir überprüfte Gemeinde setzt auch bei der Überwachung des ruhenden Verkehrs ausschließlich eigene Kräfte ein. Zu Konflikten mit den Vorgaben des Bayerischen Obersten Landesgerichtes konnte es daher bei dieser Gemeinde nicht kommen.

7.6.3 "Schwarze Listen"

Bereits in meinem 17. Tätigkeitsbericht ([Nr. 7.5.1](#)) habe ich mich mit der Eingabe eines Bürgers im Zusammenhang mit sog. "Verkehrssünderkarteien" befaßt. Dabei habe ich auf die Unzulässigkeit örtlicher Verkehrssünderkarteien bzw. sonstiger Listen oder Dateien zur Erkennung von Mehrfachtätern hingewiesen.

Durch das Urteil eines Landgerichts bin ich darauf aufmerksam geworden, daß in einer anderen Stadt eine solche Datei existieren könnte, da diese auf die Anfrage eines Gerichts sechs Fälle mitgeteilt hat, bei denen das von dem Betroffenen gehaltene Kraftfahrzeug durch Parkverstöße aufgefallen war. Diese Verstöße hatte die Stadt nach den Feststellungen des Gerichts geordnet

nach Tattag und Tatzeit, Tatort, Fahrzeug und Tatbestand in einer Datei gespeichert, in der sämtliche Verstöße aufgenommen wurden, die bei der Überwachung des ruhenden Verkehrs festgestellt werden. Die Verstöße blieben dort drei Jahre lang registriert. Das Gericht hat diese Speicherung für unzulässig gehalten und daraus ein Beweisverwertungsverbot abgeleitet. Ich habe bei dieser und einer weiteren Stadt im Rahmen datenschutzrechtlicher Prüfungen auch auf das Vorhandensein solcher Dateien geachtet und festgestellt, daß die Erkennung von Mehrfachtätern mit den jeweils eingesetzten Programmen zugleich mit der Sachbearbeitung möglich ist. Bei Eingabe eines Namens erscheinen sämtliche gespeicherten Vorgänge zu der betreffenden Person.

Ich habe gegenüber den betreffenden Gemeinden und dem Staatsministerium des Innern darauf hingewiesen, daß ich hinsichtlich der Dauer der Speicherung von Daten keine Einwendungen dagegen erhebe, daß sowohl bei der Polizei als auch den mit der eigenständigen Verkehrsüberwachung betrauten Kommunen in Verwarnungsfällen die Daten noch einige Zeit nach Bezahlung des Verwarnungsgeldes gespeichert bleiben, um z.B. die Beantwortung evtl. Nach- bzw. Rückfragen zu ermöglichen oder Fehlbuchungen nachvollziehen zu können. Bei der Polizei beträgt diese Speicherungsfrist bis zu vier Monaten, die Kommunen haben - unter Beachtung der [Art. 12 Abs. 1 und 2 BayDSG](#) - in eigener Zuständigkeit zu entscheiden, wann sie die gespeicherten Daten sperren bzw. löschen. Ein Zeitraum von vier Monaten nach Abschluß des Verfahrens sollte aber grundsätzlich nicht überschritten werden. Nach diesem Zeitpunkt sind alle Daten, die nicht dem Auffinden der Akten dienen, zu löschen oder - falls dies nicht möglich ist - zu sperren.

Der Nachweis der Mehrfachtäterschaft eines Betroffenen darf sich nicht durch Einsatz eines Programmes ergeben, das zur Sachbearbeitung bei der kommunalen Verkehrsüberwachung eingesetzt wird. Ermöglicht ein solches Programm diese Funktion und ist eine technische Sperre nicht möglich, so ist ein **Nutzungsverbot** zur Erkennung von Mehrfachtätern in die Verfahrensbeschreibung nach [Art. 26 Abs. 2 BayDSG](#) aufzunehmen. Darauf habe ich die betreffenden Gemeinden hingewiesen.

7.6.4 Lichtbildabgleich mit dem Paß- bzw. Personalausweisregister

Schon in meinem 17. Tätigkeitsbericht ([Nr. 7.5.4](#)) habe ich mich mit der Nutzung von Paßbildern in Ordnungswidrigkeitenverfahren befaßt und darauf hingewiesen, daß Paßausweisdaten nach § 22 Abs. 2 Paßgesetz und § 2 b Personalausweisgesetz nur unter den dort genannten Voraussetzungen übermittelt werden dürfen, insbesondere erst dann, wenn die Daten beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß.

Im Berichtszeitraum haben sich eine Vielzahl von Bürgerinnen und Bürgern an mich gewandt und sich über eine aus ihrer Sicht unzulässige Verwendung der Fotos aus dem Paß- bzw. Personalausweisregister beschwert. Die Überprüfung ergab, daß in der Praxis große Unsicherheiten über Anwendung und Auslegung der genannten Vorschriften bestehen, daß aber in vielen Fällen die gesetzlichen Vorgaben eingehalten worden sind.

Aus den Bestimmungen des Paß- bzw. Personalausweisgesetzes geht eindeutig hervor, daß ein **routinemäßiger Abgleich** von Paßbildern mit dem Tatortfoto der Betroffenen nicht zulässig ist. Vielmehr hat die zuständige Behörde in jedem Einzelfall zu prüfen, ob die Voraussetzungen der gesetzlichen Vorschriften erfüllt sind. In der Praxis ist vor allem die Frage von großer Bedeutung, wann davon ausgegangen werden kann, daß Daten bei dem Betroffenen nicht oder nur mit einem unverhältnismäßig hohen Aufwand erhoben werden können.

Ich halte folgendes für sachgerecht:

Richtet sich der Verdacht gegen den **Fahrzeughalter**, so hat dieser regelmäßig einen Anhörbogen erhalten. Sendet er diesen innerhalb einer angemessenen Frist nicht zurück oder äußert er sich darin nicht zur Sache, kann davon ausgegangen werden, daß eine Bereitschaft des Halters, an der Ermittlung des Täters mitzuwirken, nicht besteht. In einem solchen Fall, in dem der Betroffene Gelegenheit zur Äußerung hatte und damit eine Datenerhebung bei ihm selbst bereits erfolglos versucht wurde, halte ich einen Abgleich mit dem Paß- bzw. Personalausweisregister für zulässig.

Ist es jedoch nach den Umständen offen, ob eine Bereitschaft des Halters, an der Ermittlung des Täters mitzuwirken, besteht, so ist entsprechend der gesetzlichen Regelung zunächst zu versuchen, die Daten bei dem Betroffenen zu erheben. Äußert sich der Halter z.B. dahingehend, daß er

sich nicht mehr sicher sei, ob er selbst oder ein Dritter gefahren sei, so ist er entweder aufzusuchen, vorzuladen oder um die Übersendung eines Lichtbildes zu seiner Person zu bitten. Dies sollte am besten durch Kopie des Personalausweises erfolgen, damit die Identität der abgebildeten Person nicht zweifelhaft ist.

Richtet sich der Verdacht gegen eine bestimmte andere Person wie z.B. gegen einen bestimmten Firmenfahrer oder die Ehefrau des Fahrzeughalters, so halte ich es für unzulässig, ohne weitere Ermittlungsversuche bei der Ehefrau bzw. dem Firmenfahrer einen Lichtbildabgleich beim Paß- bzw. Personalausweisregister vorzunehmen. Betroffener ist jeweils die Person, deren Lichtbild abgeglichen werden soll. Bei dieser muß versucht werden, zu klären, ob sie mit der auf dem Beweisfoto abgebildeten Person identisch ist.

Ein unverhältnismäßig hoher Aufwand kommt nicht schon **allein** deshalb in Betracht, weil mehrere Betroffene abgeklärt werden müßten. Mein entsprechender Hinweis im 17. Tätigkeitsbericht ([Nr. 7.5.4](#)) ist so zu verstehen, daß bei einer Mehrzahl von in Frage kommenden Betroffenen eine Datenerhebung unverhältnismäßig sein **kann**, wobei es jedoch stets auf die Umstände des Einzelfalls ankommt.

Bei der Überprüfung der Einzelfälle habe ich insbesondere bei einer bayerischen Großstadt festgestellt, daß Radarfotos an das Paßamt einer Gemeinde übersandt werden, damit diese die Identität des Fahrers überprüft. Die in der Übersendung des Radarfotos liegende Datenübermittlung ist nach [Art. 18 Abs. 1 BayDSG](#) unzulässig, da nach dieser Vorschrift eine solche nur vorgenommen werden kann, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder empfangenden Stelle liegenden Aufgaben erforderlich ist.

Diese Erforderlichkeit fehlt aber, weil die ersuchende Behörde den Lichtbildabgleich ohne weiteres und ohne einen zusätzlichen Eingriff in das Persönlichkeitsrecht der Betroffenen selbst vornehmen kann, sobald ihr das angeforderte Lichtbild übersandt worden ist.

8. Gemeinden, Städte und Landkreise

8.1 Prüfungen

Bei der Prüfung von Landratsämtern und Kommunen mußte ich folgende Mängel feststellen, die - soweit nichts anderes ausgeführt ist - von den betroffenen Stellen dann selbst behoben wurden:

1. Aussonderung von Akten und Löschung von Daten

Bei meinen Prüfungen von Landratsämtern mußte ich feststellen, daß die Löschung von Daten in Akten bzw. Dateien häufig nur sehr unzureichend durchgeführt wird. Als Gründe hierfür wurden fehlende Löschungsroutrinen in den Programmen bzw. Personalmangel zum Aussondern der Akten angegeben. Ein Faktor, der vermutlich auch dazu beiträgt, daß viele Daten zu lange aufgehoben werden, ist die Tatsache, daß in älteren Programmen keine Regelfristen für die Löschung oder für die Prüfung der Löschung (vgl. [Art. 26 Abs. 2 Nr. 6 BayDSG](#)) vorgesehen werden mußten.

Soweit keine spezialgesetzlichen Vorschriften bestehen (z.B. § 6 der Ausländerdateienverordnung), sind Daten dann zu löschen, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind ([Art. 12 Abs. 1 Nr. 2, Abs. 4 Satz 2 BayDSG](#)). Um eine möglichst einheitliche Praxis der einzelnen Landratsämter zu erreichen, habe ich empfohlen, bei der Festlegung von Aussonderungsfristen, soweit sie nicht bereits durch Gesetz, Verordnung oder ggf. Bekanntmachung vorgegeben sind, die Aufsichtsbehörde und ggf. auch das zuständige Fachministerium zu beteiligen.

Um zu verhindern, daß Daten vernichtet werden, die möglicherweise archivwürdig sind, darf eine Löschung erst dann erfolgen, wenn die Unterlagen vorher einem öffentlichen Archiv zur Übernahme angeboten wurden und von diesem nicht übernommen wurden oder über die Übernahme nicht fristgerecht entschieden wurde. Dies gilt nur dann nicht, wenn die öffentliche Stelle nicht verpflichtet ist, die Unterlagen einem öffentlichen Archiv anzubieten ([Art. 12 Abs. 8 BayDSG](#)).

2. Behandlung der Akten verstorbener Waffenbesitzkarteninhaber

Bei einem der überprüften Landratsämter war es übliche Praxis, daß in Fällen, in denen der Inhaber einer Waffenbesitzkarte gestorben war, seine Akte der Akte des Erben der Waffen beigefügt wurde. Dies ist nur zulässig, wenn die Kenntnis der Akte des Verstorbenen zur Aufgabenerfüllung erforderlich ist.

Das war jedoch nicht der Fall. Der Erbe hat nach einer gewissen Übergangsfrist die Ausstellung einer eigenen Waffenbesitzkarte oder die Eintragung der Waffe in eine bereits erteilte Waffenbesitzkarte zu beantragen, sofern er die Schußwaffe nicht vorher einem Berechtigten überläßt (§ 28 Abs. 5 Satz 1 des Waffengesetzes - WaffG -). Da es sich bei der Waffenbesitzkarte um eine personenbezogene, d.h. an eine bestimmte Person gebundene Erlaubnis handelt, sind die Akten des Verstorbenen für die Erteilung einer entsprechenden Erlaubnis an den Erben nicht erforderlich.

Ich habe daher dem Landratsamt mitgeteilt, daß ich eine Beifügung dieser Akten zur Akte des Erben für unzulässig halte und diese Verfahrensweise daher künftig zu unterlassen ist. In den Fällen, in denen dies bereits in der Vergangenheit geschehen war, habe ich eine Trennung der Akten verlangt.

3. Datenübermittlung an Baustelleninformationsdienste

Ein Landratsamt, das regelmäßig Daten aus Bauanträgen an Baustelleninformationsdienste weiterleitet, sofern der Bauantragsteller dem nicht widersprochen hat, übermittelte dabei auch das Datum des Eingangs des Bauantrags. Gem. Art. 84 Satz 1 der Bayer. Bauordnung (BayBO) dürfen die Bauaufsichtsbehörden jedoch nur den Ort und die Straße einer Baustelle, Art und Größe des Bauvorhabens sowie Namen und Anschrift des Bauherrn und des Entwurfsverfassers veröffentlichen oder an Dritte zum Zwecke der Veröffentlichung übermitteln, wenn der Betroffene der Veröffentlichung nicht widersprochen hat. Die Bekanntgabe des Eingangsdatums des Bauantrags war danach unzulässig. Ich habe das Landratsamt daher aufgefordert, dies zukünftig zu unterlassen.

4. Weitergabe von Listen aller eingegangenen Gewerbeanzeigen innerhalb einer Stadt

Bei der Prüfung einer Stadt habe ich festgestellt, daß die Daten aus sämtlichen dort eingehenden Gewerbeanzeigen in Listen zusammengefaßt und an die Lebensmittelüberwachung weitergegeben werden. Diese pauschale Weitergabe an die Lebensmittelüberwachung war nicht zulässig.

Die regelmäßige Weitergabe des Namens, der betrieblichen Anschrift und der angezeigten Tätigkeit darf innerhalb der Kommune dann erfolgen, wenn dies zur Aufgabenerfüllung des Empfängers erforderlich ist (§ 14 Abs.7 Satz 1 i.V.m. Abs. 6 Satz 1 GewO). Die Übermittlung weiterer Daten aus der Gewerbeanzeige ist unter den in § 14 Abs. 6 Satz 2 GewO genannten besonderen Voraussetzungen zulässig, z.B. u.a. wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist .

Vor der Weitergabe an eine andere Stelle innerhalb der Kommune ist daher für jeden einzelnen in der Liste enthaltenen Fall stets zu prüfen, ob § 14 Abs. 6 GewO die Datenübermittlung an die konkrete Stelle erlaubt. Nur in den seltensten Fällen wird danach die Weiterleitung der gesamten Liste zulässig sein. Außerdem wird in der Regel die Übermittlung der Grunddaten (Name, betriebliche Anschrift, angezeigte Tätigkeit) für die Zwecke des Empfängers ausreichen. Soweit darüberhinaus weitere Daten benötigt werden, können diese im Einzelfall vom Gewerbesachgebiet auf Anforderung übermittelt werden, sofern § 14 Abs. 7 Satz 1 i.V.m. Abs. 6 Satz 2 GewO dies zuläßt.

Die Listen für die Lebensmittelüberwachung durften danach nur die Daten von Gewerbebetrieben enthalten, deren Tätigkeit für die Aufgabenerfüllung dieser Stelle relevant ist (z.B. durfte die Lebensmittelüberwachung die Daten der lebensmittelverarbeitenden Betriebe erhalten). Im übrigen bestand keine Veranlassung für eine generelle Übermittlung von Daten über den Namen, die betriebliche Anschrift und die angezeigte Tätigkeit hinaus. Ich habe daher die Stadt aufgefordert, den Umfang der Listen auf das zulässige Maß zu reduzieren.

8.2 Änderung des Gemeinde- und Landkreiswahlgesetzes

Nach Art. 4 Abs. 3 des Gemeinde- und Landkreiswahlgesetzes (GLKrWG) verhandeln, beraten und entscheiden die Wahlausschüsse und die Wahlvorstände in öffentlicher Sitzung. Das Gesetz sieht auch bei einem Vorliegen schutzwürdiger Interessen einzelner Personen keine Behandlung in nichtöffentlicher Sitzung vor. Berechtigten Interessen betroffener Bürger an der Geheimhaltung ihrer schutzwürdigen personenbezogenen Daten wird dadurch nicht Rechnung getragen. Das Staatsministerium des Innern hat mir dazu mitgeteilt, daß es insbesondere bei Anfragen anlässlich der letzten allgemeinen Gemeinde- und Landkreiswahlen die Auffassung vertreten hat, daß in analoger Anwendung des Art. 52 Abs. 2 GO auch hier die Grundsätze des Datenschutzes zu beachten sind. Nach meinen Erfahrungen wird in der Praxis allerdings nicht immer entsprechend verfahren. So hat mir z.B. die Presse einen Fall vorgetragen, in dem eine Stadt unter Hinweis auf Art. 4 Abs. 3 GLKrWG den Gesundheitszustand eines für den Stadtrat vorgesehenen Nachrückers, der ein ärztliches Attest vorgelegt hatte, aus dem sich ergeben hat, daß er gesundheitlich nicht in der Lage war, sein Amt anzutreten, in öffentlicher Sitzung behandelt hat. Ich rege deshalb an, Art. 4 Abs. 3 GLKrWG entsprechend der Regelung in Art. 52 Abs. 2 GO dahingehend zu ergänzen, daß die Sitzungen der Wahlausschüsse und der Wahlvorstände nichtöffentlich sind, soweit das Wohl der Allgemeinheit oder berechnigte Ansprüche einzelner dies erfordern.

8.3 Datenschutz bei Volksbegehren

Nach Art. 69 Abs. 2 des Landeswahlgesetzes muß die Eintragung in Eintragungslisten für Volksbegehren neben dem Vor- und Familiennamen auch die eigenhändige Unterschrift und das Geburtsdatum enthalten. Nach meiner Auffassung könnte auf die Angabe des Geburtsdatums verzichtet werden, denn die Identität der eintragungswilligen Person wird durch die Vorlage des Personalausweises bzw. Passes und ihre Berechnigung, am Volksbegehren teilzunehmen, durch eine Überprüfung im Wählerverzeichnis festgestellt. Durch einen Vermerk im Wählerverzeichnis (Abhaken) wird verhindert, daß sich eine Person mehrmals in die Eintragungsliste einträgt. Ich habe deshalb gegenüber dem Innenministerium angeregt, das Geburtsdatum sobald wie möglich zu streichen. Das Innenministerium hat mir daraufhin mitgeteilt, daß es den Verzicht auf

die Angabe des Geburtsdatums für die nächste Gesetzesnovelle zur Prüfung vorgemerkt hat. Aus datenschutzrechtlicher Sicht zu begrüßen wäre auch ein Verfahren, bei dem vermieden wird, daß Personen, die sich in die Eintragungsliste eintragen, Kenntnis von den Voreintragungen auf der laufenden Liste erhalten (z.B. Gestaltung der Liste als Leporello oder Abdecken der Voreintragungen). Nach der bestehenden Rechtslage darf den Stimmberechtigten zwar nur die laufende Liste vorgelegt werden (§ 80 Abs. 7 Satz 2 der Landeswahlordnung). Dabei kann jedoch nicht verhindert werden, daß sie die Namen (und bis zu einer Änderung des Landeswahlgesetzes auch das Geburtsdatum) der Personen erfahren, die sich vor ihnen eingetragen haben. Das Innenministerium vertritt dazu allerdings die Auffassung, daß ein Verfahren, mit dem zuverlässig verhindert werden könnte, daß Eintragungswillige von Voreintragungen Kenntnis erhalten, mit einem vertretbaren organisatorischen und kostenmäßigen Aufwand nicht möglich erscheine.

8.4 Datenschutz bei Bürgerbegehren

8.4.1 Inhalt der Eintragungslisten

Bei Bürgerbegehren werden die Unterschriften im Gegensatz zur Durchführung von Volksbegehren im Privatbereich gesammelt. Der Inhalt der Eintragungslisten ist gesetzlich nicht vorgegeben. Es kann deshalb bei der derzeitigen Rechtslage nicht verhindert werden, wenn Initiatoren von Bürgerbegehren in ihren Eintragungslisten das Geburtsdatum vorsehen. Wie bei den Volksbegehren ist die Angabe des Geburtsdatums aber auch in den Eintragungslisten für Bürgerbegehren nicht erforderlich. Durch eine gesetzliche Festlegung der in die Listen einzutragenden personenbezogenen Daten könnte bestimmt werden, daß das Geburtsdatum nicht erhoben und aufgenommen werden darf. In meinem 17. Tätigkeitsbericht habe ich unter der [Nr. 8.4.1](#) eine entsprechende Ergänzung der Rechtsvorschriften angeregt und in diesem Zusammenhang eine abschließende Festlegung der in die Listen einzutragenden Daten vorgeschlagen.

8.4.2 Unzulässige Auswertung von Unterschriften und unzulässige Einsichtnahme durch Dritte

Im 17. Tätigkeitsbericht habe ich unter [Nr. 8.4.2](#) darauf hingewiesen, daß die Gemeinden und Landkreise die für ein Bürgerbegehren abgegebenen Unterschriftenlisten nur hinsichtlich der Frage auswerten dürfen, ob das Bürgerbegehren von einer ausreichenden Zahl antragsberechtigter Gemeinde- bzw. Kreisbürger (Art. 18 a Abs. 6 der Gemeindeordnung; Art. 25 a Abs. 6 der Landkreisordnung) unterschrieben worden ist. Auch das Bayerische Staatsministerium des Innern hat auf meine Anregung hin die Gemeinden und die Landkreise bereits durch Rundschreiben vom 6.3.1996 auf die Beachtung des Grundsatzes der Zweckbindung bei der kommunalrechtlichen Überprüfung der Unterschriftenlisten für Bürgerbegehren hingewiesen. Gleichwohl wurden mir im Berichtszeitraum aufgrund von Bürgereingaben erneut Fälle bekannt, in denen Gemeinden bei der Auswertung der Eintragungslisten gegen den Grundsatz der Zweckbindung verstoßen haben und darüber hinaus Dritten unzulässig Einsicht in die Unterschriftenlisten gewährt haben, in einem Fall dem Bauantragsteller und Grundstückseigentümer, gegen dessen Vorhaben die Unterschriftenlisten eingereicht worden waren, in einem anderen Fall einem zufällig auf der Gemeinde vorsprechenden Bürger, der Interesse an den Listen gezeigt hat. Diese Datenschutzverstöße habe ich beanstandet.

8.5 Vorbereitung nichtöffentlicher Sitzungen der Kreisgremien

Ein Landkreis, der seine Mandatsträger in nichtöffentlicher Sitzung durch Tischvorlagen für die Sitzungsdauer informiert, hat sich an mich mit der Frage gewandt, wie die Unterrichtung der Mandatsträger im Rahmen der Vorbereitung solcher Sitzungen erfolgen sollte, um sowohl dem Informationsrecht der Mandatsträger als auch dem Recht der Betroffenen auf informationelle Selbstbestimmung Rechnung zu tragen. Ich habe dem Landkreis folgendes mitgeteilt:

Nach Art. 33 Satz 1 der Landkreisordnung (LKrO) führt der Landrat den Vorsitz im Kreistag, im Kreisausschuß und in den weiteren Ausschüssen. In seiner Eigenschaft als Vorsitzender legt der Landrat die Tagesordnung fest, beruft den Kreistag und die Ausschüsse ein und bereitet die Sitzungsgegenstände vor. Hierbei entscheidet zunächst der Landrat nach pflichtgemäßem Ermes-

sen, auf welche Weise er die Kreisräte über die zu behandelnden Beratungsgegenstände informieren will. Die Unterrichtung der Mandatsträger kann durch die Versendung von Sitzungsunterlagen, mündlichen Vortrag in der Sitzung und die Verteilung von Tischvorlagen erfolgen. Unterlagen mit Angaben zu sensiblen, in nichtöffentlicher Sitzung zu behandelnden Gegenständen, sollten nicht versandt, sondern ggf. numeriert als Tischvorlage für die Dauer der Sitzung zur Verfügung gestellt und anschließend wieder eingesammelt werden (vgl. 12. Tätigkeitsbericht 1990, Nr. 7.1, und 15. Tätigkeitsbericht 1993, Nr. 7.2, 1. Spiegelstrich, letzter Absatz, sowie Wilde/Ehmann/Niese/Knoblauch, Kommentar zum Bayer. Datenschutzgesetz, Teil C Handbuch S. 54).

Die Verfahrensweise des Landkreises im vorliegenden Fall, im Rahmen der Vorbereitung nichtöffentlicher Sitzungen die Mandatsträger durch Tischvorlagen zu informieren, die für die Dauer der Sitzung zur Verfügung gestellt werden, entspricht meinen Empfehlungen und den Empfehlungen des Bayerischen Staatsministeriums des Innern zur Behandlung von Unterlagen mit Angaben zu sensiblen, in nichtöffentlicher Sitzung zu behandelnden Gegenständen. Allerdings muß den Mitgliedern eine ordnungsgemäße Sitzungsvorbereitung ermöglicht werden, damit sie ihre Obliegenheiten gewissenhaft wahrnehmen können (vgl. Art. 14 Abs. 1 LKrO). Dies kann es im Einzelfall gebieten, daß darüber hinaus geeignete Unterlagen in einer der Bedeutung und Schwierigkeit der Angelegenheit angemessenen Zeitspanne vor der Sitzung in den Amtsräumen zur Einsichtnahme durch die Mandatsträger bereitgehalten werden oder, soweit im Einzelfall eine Einsichtnahme nicht möglich oder aus objektiven Gründen nicht zumutbar ist, die Unterlagen auch zugesandt werden, soweit dies der Sensibilität der Daten, die weitergegeben werden, Rechnung trägt und nach den Gesamtumständen vertretbar ist. Generell ist bei der Unterrichtung der Mandatsträger darauf zu achten, daß mit Rücksicht auf das Recht auf informationelle Selbstbestimmung der Betroffenen deren personenbezogene Daten nur soweit erforderlich offenbart werden und die zumutbaren Vorkehrungen zu deren Geheimhaltung getroffen werden. Kommt nach diesen Grundsätzen eine Übersendung von Sitzungsunterlagen in Betracht und zeigt die Praxis, daß Daten daraus an die Öffentlichkeit gelangen, dann ist in künftigen Fällen bei der Übersendung von Sitzungsunterlagen ein strengerer Maßstab anzulegen. Bei der Sitzungsvorbereitung gemeindlicher Gremien durch den ersten Bürgermeister nach Art. 46 Abs. 2 Satz 1 der Gemeindeordnung ist entsprechend zu verfahren.

In meinem 14. Tätigkeitsbericht habe ich mich unter 7.4 bereits zur Zulässigkeit der Aufbewah-

zung von Sitzungsunterlagen in "privaten" Akten der Mandatsträger geäußert. Dazu ergänzend weise ich in diesem Zusammenhang auf das aus Art. 100 a Abs. 2 Satz 3 BayBG resultierende Verbot der Führung unzulässiger Personal-Nebenakten hin. Ich empfehle daher dringend, ausgegebene Sitzungsunterlagen mit Personaldaten nach der Sitzung wieder einzuziehen.

8.6 Übermittlung der Höhe von Aufwandsentschädigungen an Parteien

Ein Landkreis hat sich an mich mit der Bitte um Prüfung gewandt, ob die Beträge der im Einzelfall ausbezahlten Aufwandsentschädigungen, die die Kreisräte des Kreistages für ihre ehrenamtliche Tätigkeit erhalten, örtlichen Organisationen verschiedener Parteien, die mit einem entsprechenden Wunsch an die Landkreisverwaltung herangetreten sind, bekanntgegeben werden dürfen. Die Aufwandsentschädigung setzt sich aus dem Sitzungsgeld für die Teilnahme an den Sitzungen der Kreisorgane, aus einer Fahrkostenpauschale sowie aus einem Ersatz für einen eventuellen Verdienstausschlag zusammen. Die Entschädigungssätze sind durch Satzung festgesetzt. Bei der im Einzelfall festgesetzten Aufwandsentschädigung handelt es sich um ein personenbezogenes Datum des betroffenen Kreisrates. Dieses Datum wird auf der Grundlage der in der Satzung veröffentlichten Entschädigungssätze für jeden Kreisrat individuell anhand seiner persönlichen Daten berechnet und ist deshalb schutzwürdig. Ohne Zusatzwissen ist die Höhe der jeweiligen Aufwandsentschädigung nicht feststellbar.

Da keine vorrangigen besonderen Rechtsvorschriften bestehen, richtet sich die Zulässigkeit der Datenübermittlung nach [Art. 19 Abs. 1 Nr. 2](#) des Bayerischen Datenschutzgesetzes (BayDSG). Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist danach zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

Die Rechtmäßigkeit der an die Kreisräte ausbezahlten Aufwandsentschädigung wird durch die gesetzlich dafür vorgesehenen Organe überprüft. Diese sind insbesondere der Kreistag bzw. der zuständige Ausschuß, die Aufsichtsbehörde und die Rechnungsprüfung. Darüber hinaus besteht kein berechtigtes Interesse Dritter, etwa politischer Parteien, an der Kenntnis der individuellen Aufwandsentschädigung der einzelnen Kreisräte. Diese haben vielmehr ein schutzwürdiges Interesse daran, daß ihre personenbezogenen Daten im Bereich der Verwaltung entsprechend den

gesetzlichen Bestimmungen behandelt werden und nicht Dritten zugänglich gemacht werden. Eine Übermittlung der Höhe der Aufwandsentschädigung der einzelnen Kreisräte an Parteien, bei denen es sich um nicht-öffentliche Stellen handelt, kommt somit gem. [Art. 15 Abs. 1 Nr. 2 BayDSG](#) nur mit Einwilligung der Betroffenen in Betracht.

8.7 Behandlung von Planunterlagen über Bauvorhaben in öffentlicher Sitzung

Ein Landratsamt und eine Verwaltungsgemeinschaft haben aus datenschutzrechtlicher Sicht Bedenken gegen den aus dem Bauausschuß einer Mitgliedsgemeinde geäußerten Wunsch vorgetragen, Planzeichnungen aus der Bauantragsmappe des jeweiligen Bauantragstellers zur Einsicht der Mitglieder des Bauausschusses im Rahmen der Beurteilung bzw. der Stellungnahme nach dem Baugesetzbuch an die Saalwand für die Zeitdauer der öffentlichen Sitzung anzuheften. Damit hätten die Zuhörer die Möglichkeit, Detailkenntnisse über die Planzeichnungen (z.B. Anordnung und Größe der einzelnen Wohnräume) zu erlangen. Die Bedenken waren aus den folgenden Gründen berechtigt:

Das Anheften der Planzeichnungen an der Saalwand soll der Information der Ausschußmitglieder über den Beratungsgegenstand dienen. Die Unterrichtung des Gemeinderats und seiner Ausschüsse über die in den Sitzungen zu behandelnden Gegenstände ist Aufgabe des ersten Bürgermeisters (Art. 46 Abs. 2 GO, Art. 55 Abs. 2 GO). Nach Art. 46 Abs. 2 GO bereitet der erste Bürgermeister die Beratungsgegenstände vor und beruft den Gemeinderat ein. Dabei entscheidet zunächst der erste Bürgermeister nach pflichtgemäßem Ermessen, auf welche Weise er die Mandatsträger über die zu behandelnden Beratungsgegenstände informieren will. Die Unterrichtung der Mandatsträger kann durch die Versendung von Sitzungsunterlagen, mündlichen Vortrag in der Sitzung und Verteilung von Tischvorlagen erfolgen. Insbesondere bei Planunterlagen, die für eine Versendung oder als Tischvorlage nicht in Betracht kommen, kann auch eine Einsichtnahme durch interessierte Mandatsträger vor der Sitzung in der Verwaltung oder/und während der Beratung vorgesehen werden. Denkbar ist insbesondere bei bedeutenderen Vorhaben auch eine gemeinsame Information und Einsichtnahme des Gemeinderats bzw. des zuständigen Ausschusses vor der Sitzung durch den ersten Bürgermeister.

Bei der Vorbereitung und Durchführung der Sitzungen sind die zum Schutz personenbezogener Daten erforderlichen Maßnahmen zu treffen. Das bedeutet, daß ein Anheften von Planunterlagen

an der Saalwand, das in öffentlicher Sitzung den Zuhörern die Möglichkeit geben würde, Detailkenntnisse über das Vorhaben des Bauwerbers zu erlangen, z.B. u.a. Lage und Größe eines Schlafzimmers, in der Regel in unzulässiger Weise in dessen Recht auf informationelle Selbstbestimmung eingreifen würde und deshalb zu unterbleiben hat. Demgegenüber sind schutzwürdige Interessen des Bauwerbers grundsätzlich nicht berührt, soweit lediglich Übersichtslagepläne aufgehängt werden, aus denen keine Detailinformationen zu dem Vorhaben entnommen werden können, sondern z.B. nur die Lage des Vorhabens im Vergleich zur umgebenden Bebauung ersichtlich ist. Darüber hinaus sind je nach Art des Vorhabens weitere Fälle denkbar, in denen Planunterlagen mit weitergehenden Informationen in öffentlicher Sitzung aufgehängt werden dürfen, weil das Bauvorhaben Interessen der Allgemeinheit berührt und ein schutzwürdiges Interesse des Bauwerbers an dem Ausschluß der Kenntnisnahme durch die Öffentlichkeit nicht besteht (z.B. beim Bau von Privatschulen, Lebensmittelgeschäften etc.).

Im Einzelfall ist jeweils eine Abwägung zwischen den berechtigten Interessen der Allgemeinheit und den schutzwürdigen Belangen des Bauwerbers vorzunehmen.

8.8 Anfertigung von Sitzungsniederschriften kommunaler Gremien im häuslichen Bereich

Eine Stadt hat mich um Auskunft gebeten, ob die Anfertigung von Niederschriften über öffentliche und nichtöffentliche Sitzungen der Stadtratsgremien im häuslichen Bereich durch Telearbeit zulässig ist und welche konkreten Anforderungen ggf. an technische und organisatorische Sicherungsmaßnahmen für die Telearbeitsplätze im häuslichen Bereich zu stellen sind.

Ich vertrete dazu die folgende Auffassung:

Die Weitergabe personenbezogener Daten an Bedienstete, auch wenn sie in der eigenen Wohnung arbeiten, stellt weder eine Datenübermittlung an Dritte noch eine Auftragsdatenverarbeitung durch Dritte dar. Es handelt sich um eine Nutzung von Daten innerhalb der speichernden Stelle. Soweit keine vorrangigen bereichsspezifischen Rechtsvorschriften bestehen, findet auf die Datenverarbeitung im häuslichen Bereich das Bayerische Datenschutzgesetz Anwendung. Da die Telearbeiter Bedienstete der Stadt bleiben, bleibt der Dienstherr weisungsbefugt. Er bestimmt die Art und Weise, wie die Aufgaben zu erledigen sind und welche Anforderungen an die Wohnraumarbeitsplätze zu stellen sind.

Vor diesem Hintergrund halte ich die Anfertigung auch von Niederschriften über nichtöffentliche Sitzungen der Stadtratsgremien durch Mitarbeiter(innen) der Stadt im häuslichen Bereich durch Telearbeit zwar nicht grundsätzlich für unzulässig. Die Stadt muß sich jedoch der datenschutzrechtlichen Risiken bewußt sein, wenn sie die Verarbeitung personenbezogener Daten durch städtische Bedienstete im häuslichen Bereich gestatten will. Im Hinblick auf diese Risiken empfehle ich, auf die Bearbeitung von sensitiven Daten, insbesondere von Personaldaten, im häuslichen Bereich zu verzichten. Häufig werden insbesondere auch in nichtöffentlichen Sitzungen der Gemeindegremien sensible personenbezogene Vorgänge behandelt, bei denen aus Sicherheitsgründen von einer Bearbeitung im häuslichen Bereich abgesehen werden sollte. Die Bayerischen Staatsministerien des Innern, der Finanzen und für Unterricht, Kultus, Wissenschaft und Kunst haben die Bearbeitung von Personaldaten im häuslichen Bereich durch entsprechende Weisungen bereits ausgeschlossen. Bei ihrer Entscheidung über die Gestattung von Telearbeit mit sensiblen Daten im häuslichen Bereich sollte die Stadt auch die örtlichen Verhältnisse und die der beteiligten Bediensteten berücksichtigen. Zu den Sicherheitsanforderungen an Telearbeitsplätze habe ich in meinem 17. Tätigkeitsbericht 1996 unter [Nr. 18.3.3](#) Stellung genommen.

8.9 Veröffentlichung von Niederschriften über öffentliche Sitzungen des Gemeinderats im Internet

In der Presse wurde über folgenden Vorgang berichtet: Ein Gemeinderatsmitglied hatte zunächst mit Zustimmung der Gemeinde auf seiner Homepage im Internet eine allgemeine Information über die Gemeinde veröffentlicht. Ohne die Zustimmung der Gemeinde veröffentlichte das Gemeinderatsmitglied dann jedoch die amtlichen Sitzungsniederschriften über öffentliche Sitzungen des Gemeinderats. Die Gemeinde hat nach Beratung durch das Landratsamt ihre Zustimmung widerrufen. Das betroffene Gemeinderatsmitglied fühlte sich dadurch in seiner Meinungs- und Pressefreiheit beeinträchtigt. Ich vertrete dazu die folgende Auffassung:

1. Veröffentlichung persönlicher Notizen oder Berichte von Zuhörern oder Gemeinderatsmitgliedern

Nach Art. 52 Abs. 2 der Gemeindeordnung sind Gemeinderatssitzungen öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche

einzelner entgegenstehen. Zu öffentlichen Gemeinderatssitzungen hat grundsätzlich jedermann Zutritt. Den Zuhörern kann dabei nicht verwehrt werden, sich Notizen zu machen und diese in der öffentlichen Sitzung gefertigten persönlichen Notizen und einen daraus aus dem Gedächtnis geschriebenen Bericht im Internet zu veröffentlichen. Dies gilt auch für ein Gemeinderatsmitglied, das in öffentlicher Sitzung Notizen anfertigt, soweit sich diese auf Vorgänge beschränken, die in der öffentlichen Sitzung auch zur Sprache gekommen sind. Unzulässig wäre es, wenn das Gemeinderatsmitglied internes Zusatzwissen über einzelne Vorgänge (z.B. aus den Sitzungsunterlagen) veröffentlichen würde. Es muß jedoch bei der Veröffentlichung klar werden, daß es sich um persönliche Notizen eines zuhörenden Bürgers oder eines Gemeinderatsmitglieds, nicht aber um eine Veröffentlichung der Gemeinde oder eine amtliche Niederschrift handelt.

2. Veröffentlichung der amtlichen Niederschrift

Derartige Niederschriften sind offizielle Dokumente der Gemeinde mit dem Charakter öffentlicher Urkunden. Veröffentlichungen sind nur durch die Gemeinde, jedenfalls aber nur mit ihrer Zustimmung zulässig. Ich habe mich in meinem 14. Tätigkeitsbericht zur Veröffentlichung amtlicher Sitzungsniederschriften geäußert. Ich halte danach die Veröffentlichung der Niederschriften öffentlicher Sitzungen, die nur den Mindestinhalt des Art. 54 Abs. 1 GO enthalten, im gemeindlichen Mitteilungsblatt und die Weitergabe derartiger Niederschriften an die örtliche Presse für zulässig. Nach Auffassung des Innenministeriums ist die Veröffentlichung der amtlichen Niederschrift einer öffentlichen Sitzung des Gemeinderats durch die Gemeinde oder mit ihrer Zustimmung auch im Internet jedenfalls dann zulässig, wenn nur der Mindestinhalt nach Art. 54 Abs. 1 GO darin enthalten ist.

Aus datenschutzrechtlicher Sicht ist allerdings darauf hinzuweisen, daß bei einer Veröffentlichung im Internet weltweit eine automatisierte Auswertung der Niederschriften nach verschiedenen Suchkriterien, die beliebig miteinander verknüpft werden können, möglich ist. Bei einer Einstellung auch nur des Mindestinhalts der Niederschriften nach Art. 54 Abs. 1 GO können Anwesenheitsprofile einzelner Gemeinderatsmitglieder ange-

fertigt werden. Auch die behandelten Sitzungsgegenstände werden häufig personenbezogene Angaben von Antragstellern und Eingabeführern enthalten, die über eine Einstellung der Sitzungsniederschriften in das Internet wesentlich leichter von Dritten weltweit gesammelt und ausgewertet werden können, als bisher mit der Bekanntgabe über ein herkömmliches Medium. Dies zeigt, daß die Veröffentlichung im Internet mit einer neuen Qualitätsstufe des Eingriffs in das Recht auf informationelle Selbstbestimmung verbunden ist.

Bei einer Einspeisung von Daten aus Niederschriften über öffentliche Gemeinderatssitzungen in das Internet bestehen auch Gefahren für die Datensicherheit. Es kann nicht sichergestellt werden, daß **jederzeit** die vollständigen und unverfälschten Daten auf dem Internet-Server zum Abruf bereitgehalten werden. Es besteht die Gefahr, daß die auf dem Internet-Server gespeicherten Daten verändert, zumindest teilweise unterdrückt oder gelöscht werden. In diesem Zusammenhang können auch haftungsrechtliche Fragen nicht ausgeschlossen werden, die auf eine Gemeinde bei einer amtlichen Veröffentlichung oder einer Veröffentlichung mit Zustimmung zukommen könnten.

Die Gemeinden müssen bei ihrer Entscheidung, ob sie Niederschriften im Internet veröffentlichen, diese Risiken berücksichtigen. Das Innenministerium hat auf meine Bitte hin die nachgeordneten Behörden mit Rundschreiben darauf hingewiesen.

8.10 Akteneinsicht durch ein Stadtratsmitglied und Weitergabe personenbezogener Daten an die Presse

Ein Ehepaar hat mich um datenschutzrechtliche Überprüfung der Einsichtnahme eines Stadtratsmitglieds in die die Petenten betreffenden Vergabe- und Sanierungsakten der Stadt und der Weitergabe personenbezogener Daten aus diesen Akten an die Presse gebeten. Der Eingabe lag folgender Sachverhalt zugrunde.

Ein Stadtratsmitglied, das in seiner Funktion als Mitglied des Bauausschusses Vergabelisten erhalten hatte, nahm im Stadtplanungsamt Einsicht in die die Petenten betreffenden Vergabe- und Sanierungsakten. Seine Feststellungen aus der Akteneinsicht faßte das Stadtratsmitglied in einem Schreiben an den Oberbürgermeister zusammen. In dem Schreiben, das das Stadtratsmitglied

dem Oberbürgermeister am gleichen Tag übergab, wurde dieser außerdem um eine Überprüfung der Angelegenheit durch das Rechnungsprüfungsamt gebeten. Der Oberbürgermeister leitete das Schreiben ebenfalls noch am gleichen Tag dem Rechnungsprüfungsamt zu. Zwei Tage später berichtete die örtliche Zeitung über die Angelegenheit, wobei sie aus dem Schreiben wörtlich zitierte. Ich habe die Vorgänge datenschutzrechtlich wie folgt bewertet:

1. **Akteneinsicht durch das Stadtratsmitglied**

Dazu vertrete ich mit dem Staatsministerium des Innern, das ich um Stellungnahme gebeten hatte, folgende Auffassung: Nach Art. 30 Abs. 3 GO überwacht der Gemeinderat die gesamte Gemeindeverwaltung, insbesondere auch die Ausführung seiner Beschlüsse. Dieses Überwachungsrecht steht nach ständiger Rechtsprechung (vgl. z.B. VGH n.F. 24, 129; Fundstelle 1990, Rdn. 22; BayVBl 1990, 278; BayVBl 1990, 284) nur dem Gemeinderat als ganzem, nicht einzelnen Gemeinderatsmitgliedern oder Fraktionen zu. Ein allgemeines Auskunftsrecht, wie es in Art. 23 Abs. 2 Satz 2 LKrO nominiert ist, gibt es in der Gemeindeordnung nicht. Der VGH hat in seiner Entscheidung vom 6.9.1989 (BayVBl 1990, 278) festgestellt, daß ein einzelnes Gemeinderatsmitglied auch dann keinen gerichtlich einklagbaren Anspruch darauf hat, von der Gemeindeverwaltung bestimmte Informationen zu erlangen, wenn diese der Vorbereitung bestimmter Beschlüsse dienen sollen. Dieses Überwachungsrecht und damit das Recht auf Akteneinsicht kann der Gemeinderat einzelnen Gemeinderatsmitgliedern aber für bestimmte Aufgabengebiete oder für Einzelfälle übertragen. Es handelt sich dabei um abgeleitete Befugnisse; das einzelne Gemeinderatsmitglied nimmt das Überwachungsrecht des Gemeinderats für den Gemeinderat wahr. Die Übertragung kann durch einen gesonderten Beschluß oder durch die Geschäftsordnung erfolgen.

Im vorliegenden Fall hatte der Stadtrat dem Stadtratsmitglied, das Akteneinsicht in die Vergabe- und Sanierungsakten der Petenten genommen hatte, das Recht auf Akteneinsicht weder für den konkreten Einzelfall noch für ein bestimmtes Aufgabengebiet übertragen, zu dem die vorgenommene Akteneinsicht gehört hätte. Die sonach unzulässige Akteneinsicht habe ich beanstandet.

2. Datenübermittlung an die Presse

Die datenschutzrechtliche Überprüfung hat ergeben, daß die Weitergabe des Schreibens bzw. dessen Inhalts ausschließlich aus der öffentlichen Stelle Stadt erfolgt sein konnte. Die Weitergabe des Schreibens an die Presse war unzulässig. Die Petenten hatten ein schutzwürdiges Interesse daran, daß ihre personenbezogenen Angaben, die der Stadt im Rahmen ihrer Aufgabenerfüllung bekannt geworden sind, nicht Dritten zugänglich gemacht werden. Sie mußten darauf vertrauen können, daß ihre Angelegenheiten in der Kommune entsprechend den einschlägigen gesetzlichen Bestimmungen behandelt werden und im Bereich der Verwaltung und der zuständigen Entscheidungsgremien verbleiben. Die unzulässige Weitergabe des Schreibens habe ich ebenfalls beanstandet.

8.11 Weitergabe von Rechnungsprüfungsberichten an die Presse

Unter der Überschrift "Sanierung: Prüfer stellen zu hohe Honorare fest" berichtete eine örtliche Zeitung unter Angabe konkreter Einzelheiten, mehrfach mit wörtlichen Zitaten, und unter namentlicher Nennung betroffener Personen über den Inhalt von Prüfberichten eines städtischen Rechnungsprüfungsamtes, die sich mit der Vergabepraxis der städtischen Bauverwaltung befassen. Die Prüfberichte waren nur zwei Tage nach der Veröffentlichung in der Presse zur Behandlung in nichtöffentlicher Sitzung des städtischen Rechnungsprüfungsausschusses vorgesehen. Die von dem Pressebericht betroffenen Bürger haben sich an mich mit der Bitte um datenschutzrechtliche Überprüfung der Angelegenheit gewandt.

Die daraufhin durchgeführten Ermittlungen haben zwar nicht zur Feststellung der Person geführt, die die Berichte weitergegeben hat, so daß diese dafür nicht zur Verantwortung gezogen werden konnte. Nach dem Sachverhalt stand jedoch fest, daß es sich um eine Person handelte, die der öffentlichen Stelle Stadt zuzurechnen war, d.h. um ein Mitglied des Rechnungsprüfungsausschusses oder einen sonstigen Angehörigen der Stadt.

Die Datenweitergabe war rechtswidrig. Die Berichte des Rechnungsprüfungsamtes enthielten Informationen über Auftragsvergaben und Honorarzahlungen an einen Bürger sowie Sanierungsmaßnahmen eines Ehepaars, die als persönliche Angelegenheit der Betroffenen nicht an die Presse hätten weitergegeben werden dürfen. Am Erhalt von für eine nichtöffentliche Sitzung

eines Rechnungsprüfungsausschusses bestimmten Berichten kann die Presse ein berechtigtes Interesse im Sinn von [Art. 19 Abs. 1 Nr. 2 BayDSG](#) nicht geltend machen. Dem kann auch nicht entgegen gehalten werden, daß die Öffentlichkeit ein Recht darauf habe, über das Ergebnis der Überprüfung von Vorwürfen gegen die Vergabepraxis der Stadt informiert zu werden. Dieses Recht beinhaltet jedenfalls nicht die unauthorisierte Weitergabe vertraulicher Berichte des Rechnungsprüfungsamtes mit den darin enthaltenen Detailinformationen über Bürger, noch dazu vor der Behandlung in dem zuständigen Gremium. Die Weitergabe der Berichte erfolgte damit unter Verstoß gegen datenschutzrechtliche Vorschriften und wurde von mir beanstandet.

8.12 Behandlung von Grundstücksangelegenheiten in öffentlicher Gemeinderatssitzung

Eine Bürgerin, die ihrer Gemeinde ein Grundstück zum Kauf angeboten hatte, hat sich bei mir darüber beschwert, daß die Gemeinde die Angelegenheit in öffentlicher Gemeinderatssitzung behandelt hat. Die Gemeinde begründete die Behandlung in öffentlicher Sitzung damit, daß man der Petentin bei der Suche nach einem Kaufinteressenten habe behilflich sein wollen, nachdem die Gemeinde am Grunderwerb nicht interessiert gewesen sei. In Zukunft würden Grundstücksangelegenheiten jedoch nur noch in nichtöffentlicher Gemeinderatssitzung behandelt werden. Die Behandlung der Grundstücksangelegenheit der Petentin in öffentlicher Gemeinderatssitzung war unzulässig und wurde von mir deshalb beanstandet. Der Gemeinde habe ich dazu folgendes mitgeteilt:

Die Sitzungen eines Gemeinderats sind öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche einzelner entgegenstehen (Art. 52 Abs. 2 Satz 1 GO). Grundstücksangelegenheiten sind regelmäßig in nichtöffentlicher Sitzung zu behandeln. Dies gilt auch für Grundstücksverkäufe, bei denen der Gemeinderat über die Ausübung eines Vorkaufsrechts berät. Grundstücksangelegenheiten sind wegen des Geheimhaltungsinteresses und der persönlichen Belange der Beteiligten nicht geeignet in öffentlicher Sitzung behandelt zu werden (vgl. Bekanntmachung des Bayer. Staatsministeriums des Innern vom 8. Oktober 1991, Nr. I B 1-3002-3/8(91), AllMBI 1991, S. 812).

Das Argument der Gemeinde, man habe der Petentin bei der Suche nach einem Kaufinteressenten behilflich sein wollen und deshalb die Angelegenheit in öffentlicher Gemeinderatssitzung behandelt, ändert nichts daran, daß damit schutzwürdige Belange der Petentin verletzt wurden.

8.13 Online-Zugriff durch den ersten Bürgermeister einer Mitgliedsgemeinde auf Datenbestände der Verwaltungsgemeinschaft

Eine Verwaltungsgemeinschaft hat sich an mich mit der Frage gewandt, ob der erste Bürgermeister einer Mitgliedsgemeinde Datenbestände der Verwaltungsgemeinschaft durch einen Online-Zugriff von zu Hause aus nutzen kann. Ich vertrete dazu die folgende Auffassung:

- 1. Die Datenweitergabe innerhalb einer Gemeinde und zwischen einer Verwaltungsgemeinschaft und ihren Mitgliedsgemeinden ist eine Datennutzung, die sich, soweit keine bereichsspezifischen Rechtsvorschriften bestehen, nach [Art. 17 BayDSG](#) beurteilt.**

Die Weitergabe personenbezogener Daten innerhalb einer Gemeinde und zwischen einer Verwaltungsgemeinschaft und ihren Mitgliedsgemeinden ist eine Datennutzung nach [Art. 4 Abs. 7 BayDSG](#). Für den Geltungsbereich des Melderechts ergibt sich das unmittelbar aus Art. 31 Abs. 7 Satz 2 MeldeG. Soweit keine vorrangigen besonderen Rechtsvorschriften bestehen ist die Datennutzung durch den ersten Bürgermeister einer Gemeinde nach [Art. 17 BayDSG](#) zu beurteilen. Sie ist danach zulässig, soweit sie zur Durchführung der Aufgaben des Bürgermeisters erforderlich ist ([Art. 17 Abs. 1 Nr. 1 BayDSG](#)) und entweder für Zwecke erfolgt, für die die Daten erhoben bzw. gespeichert worden sind ([Art. 17 Abs. 1 Nr. 2 BayDSG](#)), oder einer der in [Art. 17 Abs. 2 bis 5 BayDSG](#) geregelten Fälle vorliegt. Nach [Art. 17 Abs. 3 Satz 1 BayDSG](#) gilt die Wahrnehmung von Aufsichts- und Kontrollbefugnissen nicht als Zweckänderung.

- 2. Ein Direktzugriff des ersten Bürgermeisters ist auf Datenbestände der Gemeinde zulässig, die er zur Aufgabenerfüllung im Rahmen eigener Sachbearbeitung benötigt und darüber hinaus allenfalls auf einen eingeschränkten Grunddatenbestand des Gemeindepersonals und der Gemeindegewohner.**

Der erste Bürgermeister vertritt die Gemeinde nach außen und leitet die Verwaltung. Nach Art. 37 Abs. 4 GO führt er zudem die Dienstaufsicht über die Beamten, Angestellten und Arbeiter der Gemeinde. Zur Wahrnehmung der Dienstaufsicht, der Behördenleitung und der Vertretung der Gemeinde nach außen ist ein umfassender Direktzugriff des

ersten Bürgermeisters auf die Datenbestände der Gemeinde nicht erforderlich. Der Bürgermeister kann sich dazu, soweit es im Einzelfall erforderlich ist, informieren und jederzeit die einschlägigen Akten vorlegen lassen. Zur Erfüllung dieser Aufgaben ist insoweit allenfalls ein Direktzugriff des ersten Bürgermeisters auf einen eingeschränkten Grunddatenbestand des Gemeindepersonals (z.B. Name, Anschrift, evtl. Geburtsdatum) und der Gemeindeeinwohner im Umfang einer einfachen Melderegisterauskunft erforderlich.

Darüber hinaus ist ein Direktzugriff im Online-Verfahren auf Datenbestände der Gemeinde durch den ersten Bürgermeister zulässig, soweit dieser Aufgaben nicht delegiert hat, sondern selbst in eigener Zuständigkeit wahrnimmt und im Rahmen der Sachbearbeitung diese Datenbestände ständig benötigt.

- 3. In einer Verwaltungsgemeinschaft ist eine Datenweitergabe zur Aufgabenerfüllung an einen Bürgermeister einer Mitgliedsgemeinde nur aus dem Datenbestand seiner Mitgliedsgemeinde zulässig.**

In einer Verwaltungsgemeinschaft ist der Aufgabenbereich der Bürgermeister der Mitgliedsgemeinden, die nicht gleichzeitig Gemeinschaftsvorsitzende sind, im Vergleich zu den Bürgermeistern von Einheitsgemeinden eingeschränkt (vgl. insbesondere Art. 4, 6 und 7 VGemO). In diesem Zusammenhang muß auch darauf hingewiesen werden, daß die Datenbestände bei der Verwaltungsgemeinschaft getrennt nach den einzelnen Mitgliedsgemeinden geführt werden müssen und eine Datenweitergabe zur Aufgabenerfüllung an den Bürgermeister einer Mitgliedsgemeinde nur aus dem Datenbestand seiner Mitgliedsgemeinde zulässig ist (vgl. [Nr. 9.3](#) meines 17. Tätigkeitsberichts 1996 zur Weitergabe von Melderegisterdaten der Verwaltungsgemeinschaften an Mitgliedsgemeinden).

4. Es ist zur Aufgabenerfüllung regelmäßig nicht erforderlich, daß der Behördenleiter alle von verschiedenen Dienststellen über denselben Bürger gespeicherten Daten kennt.

Im Zusammenhang mit der Frage der Einrichtung von Online-Zugriffen für Behördenleiter auf Dateien mit personenbezogenen Daten muß generell berücksichtigt werden, daß damit das Recht der betroffenen Personen auf informationelle Selbstbestimmung in besonderer Weise berührt sein kann. Einmal, weil damit der Kreis der Personen, die die erhöhte Verfügbarkeit der Daten in der automatisierten Datei nutzen können, um Personen erweitert wird, die in die laufende Arbeitsabwicklung des jeweiligen Amtes oder Sachgebiets normalerweise nicht eingebunden sind. Zum anderen, weil für den Behördenleiter ein Direktzugriff auf Bürgerdaten aus verschiedenen Bereichen (z.B. in einer Gemeinde aus Steuer- und Sozialdaten, aus Dateien des Ordnungsamtes oder des Melderegisters) möglich wäre. Je nach Umfang der Automatisierung in der Verwaltung könnte dies dazu führen, daß damit ein recht weitgehendes Datenprofil bestimmter einzelner Einwohner abrufbar wäre. Es ist zur Aufgabenerfüllung des Behördenleiters aber regelmäßig nicht erforderlich, daß dieser alle von verschiedenen Dienststellen über denselben Bürger gespeicherten Daten - und das auch noch im Direktzugriff - kennt.

5. Sicherheitsanforderungen bei Online-Zugriffen von zu Hause aus

Soweit ein Online-Zugriff von zu Hause aus nach Vorstehendem zulässig wäre (eingeschränkt auf die zur konkreten Aufgabenerfüllung erforderlichen Daten), sind folgende Sicherheitsmaßnahmen einzuhalten:

- Absicherung des Wählleitungszugangs (wohl über ISDN-Verbindung) gegen unberechtigte Eindringlinge in das Computersystem der Verwaltungsgemeinschaft
- Absicherung des Online-Zugriffs durch Benutzerkennung und Paßwort

- Verhinderung des Zugriffs auf die gespeicherten Daten durch unbefugte Dritte (z.B. Familienangehörige) durch geeignete Zugriffsschutzsoftware
- Verhinderung eines dezentralen Schattendatenbestands auf dem von der Verwaltungsgemeinschaft dem betreffenden Bürgermeister bereitgestellten PC durch organisatorische Maßnahmen (z.B. Nutzungsrichtlinien)
- Einsatz eines Virens scanners
- Bei Zugriff auf sensible Daten kann zudem eine Verschlüsselung der Daten (etwa durch Router) gegen Abhörer auf dem Übertragungsweg erforderlich werden.

8.14 Herausgabe von Adressenlisten für Einladungen zu Veranstaltungen

Gemeinden führen zur Vorbereitung ihrer Veranstaltungen häufig Adressenlisten sogenannter "Repräsentanten des öffentlichen Lebens". In diesen Listen sind i.d.R. der Name, der Vorname, die Funktion und oft auch die Dienstanschrift enthalten. Manchmal ist statt der Dienstanschrift die Privatadresse vermerkt. Gemeinden, die die datenschutzrechtliche Zulässigkeit der Weitergabe einer solchen Liste bzw. von Daten daraus an Dritte zu prüfen haben, die die Informationen für Einladungen zu bestimmten Veranstaltungen haben wollen, müssen folgendes beachten:

1. Rechtsgrundlage für die Datenübermittlung

Die Weitergabe der vollständigen oder auszugsweisen Adressenliste an Dritte ist eine Datenübermittlung nach [Art. 4 Abs. 6 Nr. 3 lit. a BayDSG](#). Mangels einer bereichsspezifischen Regelung richtet sich die Datenübermittlung nach den Vorschriften des Bayerischen Datenschutzgesetzes. Rechtsgrundlage für die Weitergabe der Adressenliste an andere öffentliche Stellen ist [Art. 18 BayDSG](#). Die Weitergabe an nicht-öffentliche Stellen richtet sich nach [Art. 19 Abs.1 Nr. 2 BayDSG](#).

2. Datenübermittlung an andere öffentliche Stellen

Die Gemeinden führen die Adressenliste für repräsentative Anlässe, Veranstaltungen und

Empfänge. Die Datenweitergabe an eine andere öffentliche Stelle zu einem dieser Zwecke wäre keine Zweckänderung, soweit die Adressen aus allgemein zugänglichen Quellen und damit ohne bestimmte Zweckänderung entnommen worden sind. Da eine Datenweitergabe nach [Art. 18 Abs. 1 BayDSG](#) nur zulässig ist, wenn sie zur Aufgabenerfüllung erforderlich ist, wäre allerdings vor jeder einzelnen Weitergabe zu prüfen, ob die vollständige Liste oder nur Auszüge davon weitergegeben werden dürfen.

Etwas anderes gilt für die Daten, die die Gemeinde bei den Betroffenen erhoben hat. Diese haben ihre Daten der Stadt mitgeteilt, um von dieser zu Veranstaltungen eingeladen zu werden. Die Übermittlung dieser Daten durch die Stadt an andere öffentliche Stellen wäre eine Zweckänderung, für die es in [Art. 17 Abs. 2 - 4 BayDSG](#) keine Ausnahme gibt. Die Übermittlung dieser Daten ohne Einwilligung der Betroffenen wäre daher unzulässig.

3. Datenübermittlung an nicht-öffentliche Stellen

Die Weitergabe der vollständigen oder auszugsweisen Adressenliste an nicht-öffentliche Stellen ist nach [Art. 19 Abs. 1 Nr. 2 BayDSG](#) zulässig, wenn der Auskunftersuchende ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die Betroffenen kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung haben. Ein schutzwürdiges Interesse am Ausschluß der Übermittlung ist dabei immer in den Fällen anzunehmen, in denen Personen ihre Daten der Stadt mitgeteilt haben, um von dieser eingeladen zu werden. In den übrigen Fällen, in denen die Stadt die Daten aus allgemein zugänglichen Quellen entnommen hat, muß in jedem Einzelfall geprüft werden, ob ein schutzwürdiges Interesse des jeweils Betroffenen vorliegt, das einer Übermittlung seiner personenbezogenen Daten an den anfragenden privaten Dritten zu dem genannten Zweck entgegensteht.

4. Zweckbindung

Eine Datenweitergabe ist mit der Auflage zu versehen, daß die Daten nur zu dem übermittelten Zweck verwendet werden dürfen.

5. Keine Übermittlung von Privatanschriften

Gegen die Übermittlung von Privatanschriften bestehen erhebliche datenschutzrechtliche Bedenken. Gerade Repräsentanten des öffentlichen Lebens sind oftmals Belästigungen oder Gefahren für ihre eigene Sicherheit oder die ihrer Angehörigen ausgesetzt. Das Melderecht sieht z.B. vor, daß in solchen Fällen eine Auskunftssperre eingetragen werden kann (Art. 34 Abs. 5 MeldeG). Die Weitergabe der Adressenliste mit der Privatanschrift könnte z.B. zur Umgehung einer melderechtlichen Auskunftssperre führen.

6. Einholung einer Einwilligung

Aus datenschutzrechtlicher Sicht zu empfehlen ist die Einholung einer Einwilligung der Betroffenen ([Art. 15 Abs. 1 Nr. 2 BayDSG](#)). Da eine Einwilligung für jeden Einzelfall wegen des damit verbundenen Aufwandes in der Regel nicht in Betracht kommen dürfte, bietet sich eine generelle Einwilligung für künftige Fälle an, wobei differenziert werden könnte (z.B. nach öffentlichen Stellen, Wirtschaftsverbänden etc.).

7. Keine Rechtspflicht zur Datenübermittlung

Die Datenübermittlung an andere öffentliche Stellen und an private Dritte ist unter den o.g. Voraussetzungen zulässig. Eine Rechtspflicht zur Datenübermittlung an Private besteht hingegen nicht, auch wenn die Voraussetzungen für eine Datenübermittlung im Einzelfall vorliegen.

8.15 Weitergabe eines nichtanonymisierten Urteils durch eine Gemeinde an einen Dritten

Eine Gemeinde sandte einem Bürger, mit dem sie einen Rechtsstreit führte, zur Untermauerung ihrer Rechtsauffassung ein Urteil zu, das sie in einem vergleichbaren anderen Fall erstritten hatte. Die Gemeinde hatte das Urteil vor der Versendung an den Bürger allerdings nicht anonymisiert. Ich nehme diesen Datenschutzverstoß, den mir der Bürger mitgeteilt hat, zum Anlaß, darauf hinzuweisen, daß Urteile und Beschlüsse, die die Gerichte zulässigerweise in nichtanonymisierter Form an Berechtigte versandt haben, von diesen vor einer Weitergabe an Dritte anonymisiert werden müssen.

8.16 Nachweis der Namensänderung der Schuldnerin im Zwangsvollstreckungsverfahren durch eine erweiterte Melderegisterauskunft

Eine Inkasso-Gesellschaft wollte im Rahmen einer Zwangsvollstreckung von einer Stadt einen Familienbuchauszug zum Nachweis einer Namensänderung der Schuldnerin. Die Namensänderung wegen Eheschließung war nach der Erteilung des Vollstreckungstitels erfolgt. Die Stadt hat die Ausstellung der Personenstandsurkunde abgelehnt und mir den Vorfall im Hinblick auf vermutete weitere derartige Anträge dieser und anderer Inkasso-Gesellschaften mitgeteilt. Ich weise dazu auf folgendes hin:

Die Zulässigkeit der Einsicht in Personenstandsbücher, die Durchsicht dieser Bücher und die Erteilung von Personenstandsurkunden beurteilt sich nach § 61 Personenstandsgesetz (PStG). Nach § 61 Abs. 1 PStG haben nur Personen, auf die sich der Eintrag bezieht, sowie deren Ehegatten, Vorfahren oder Abkömmlinge ein Recht auf Erteilung von Personenstandsurkunden, andere Personen nur dann, wenn sie ein **rechtliches** Interesse glaubhaft machen können. Ein rechtliches Interesse setzt voraus, daß ein Rechtsanspruch nur mit Hilfe der beantragten Personenstandsurkunde verwirklicht werden kann. Im Rahmen einer Zwangsvollstreckung kann der Gläubiger den Nachweis der Namensänderung des Schuldners auch über die erweiterte Melderegisterauskunft nach Art. 34 Abs. 2 MeldeG führen. Die erweiterte Melderegisterauskunft läßt bei Glaubhaftmachung eines berechtigten Interesses, das hier zweifellos vorliegt, eine Auskunft aus dem Melderegister über frühere Vor- und Familiennamen und frühere Anschriften zu. Sie enthält im Gegensatz zu Personenstandsurkunden (Heiratsurkunde, beglaubigte Abschrift oder Auszug aus dem Familienbuch der neuen Ehe) nur die Daten des Schuldners und nicht die Personenstandsdaten von Verwandten und angeheirateten Personen, die mit dem Schuldverhältnis nichts zu tun haben. Die Melderegisterauskunft erfüllt auch die Erfordernisse an eine öffentliche Urkunde im Sinn des § 415 ZPO. Die Stadt hat somit die Ausstellung der Personenstandsurkunde zu Recht abgelehnt, verbunden mit dem Hinweis an die Inkasso-Gesellschaft auf die Möglichkeit, eine erweiterte Melderegisterauskunft zu beantragen.

Ich weise in diesem Zusammenhang auch auf den Beschluß des Landgerichts Braunschweig vom 08.11.1994 - 8 T 459/94 - hin, in dem in einem vergleichbaren Fall u.a. folgendes ausgeführt wird: "Die von der weiteren Beteiligten zu 1) betriebene Zwangsvollstreckung gegen die Schuldnerin darf gem. § 750 Abs. 1 ZPO u.a. nur beginnen, wenn die Person, für und gegen die sie stattfinden soll, in dem Urteil oder in der ihm beigefügten Vollstreckungsklausel namentlich

bezeichnet ist. Eine nach Titelerteilung erfolgte Namensänderung des Schuldners muß der Gläubiger in öffentlicher Urkunde nachweisen. Hierzu bedarf es aber im vorliegenden Fall nicht der Erteilung einer Heiratsurkunde oder der Abschrift aus dem Familienbuch für die Schuldnerin. Vielmehr kann die weitere Beteiligte zu 1) als Gläubigerin bei Glaubhaftmachung eines berechtigten Interesses vom Meldeamt die Erteilung einer erweiterten Auskunft aus dem Melderegister nach § 33 Abs. 2 des Nds. Meldegesetzes vom 02.07.1985 (Nds. GVBl. S. 1) verlangen. Diese Vorschrift sieht die erweiterte Melderegisterauskunft auch über frühere Vor- und Familiennamen und frühere Anschriften vor. Mit diesen Auskünften in einer amtlichen Melderegisterauskunft kann die Gläubigerin den Nachweis der Identität zwischen der Person, gegen die sich der Vollstreckungstitel richtet, und der Person, gegen die vollstreckt werden soll, erbringen. Ihrem rechtlichen Bedürfnis ist somit Rechnung getragen, so daß ein weitergehender Eingriff in die Rechtssphäre der Schuldnerin durch Ausstellung einer Heiratsurkunde nicht in Betracht kommt, zumal diese Urkunde auch persönliche Daten enthält, die Außenstehende nichts angehen".

8.17 Datenübermittlung im Rahmen der Ahnen- und Familienforschung

Eine ganze Reihe von Eingaben im abgelaufenen Berichtszeitraum hat sich wieder einmal mit der Frage nach der Zulässigkeit von Auskünften im Rahmen der Ahnen- und Familienforschung beschäftigt. Als besonderes Hindernis erweist sich dabei immer wieder das Personenstandsrecht, das Auskünfte aus den Personenstandsbüchern nur unter den engen Voraussetzungen des § 61 Abs. 1 des Personenstandsgesetzes (PStG) erlaubt. Danach kann die Einsicht in Personenstandsbücher, die Durchsicht dieser Bücher und die Erteilung von Personenstandsurkunden nur von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen, also von Verwandten in gerader Linie. Andere Personen haben nur dann ein Recht hierzu, wenn sie ein rechtliches Interesse glaubhaft machen können. Die Familienforschung stellt jedoch kein solches Interesse dar. Dies wurde von der Rechtsprechung mehrfach bestätigt.

Die strengen Bestimmungen des § 61 Abs. 1 PStG gelten neben den Personenstandsbüchern auch für die vom 01.01.1876 an geführten Zivilstandsregister (Standesregister). Auf die Zivilstandsregister, die bereits vor diesem Zeitpunkt geführt wurden, findet diese Vorschrift dagegen keine Anwendung.

Inzwischen gibt es aber Initiativen zu diesem Problem. Nach dem Vorentwurf eines Fünften Gesetzes zur Änderung des Personenstandsgesetzes soll auf Anregung des Bundesbeauftragten für den Datenschutz, die ich unterstütze, § 61 Abs. 1 PStG dahingehend geändert werden, daß für eine Auskunft aus einem bzw. eine Einsicht in einen Personenstandseintrag die Glaubhaftmachung eines berechtigten Interesses genügt, wenn seit dem Tod des Betroffenen mindestens 30 Jahre oder, falls der Todestag nicht bekannt ist, seit der Geburt mindestens 120 Jahre vergangen sind.

Aus der Sicht des Datenschutzes ist eine Begrenzung auf ein "rechtliches" Interesse in den genannten Fällen nicht erforderlich. Ich würde es deshalb sehr begrüßen, wenn diese Beschränkung in der genannten Weise geändert würde, da damit ein ungerechtfertigter Vorwurf gegen den Datenschutz ausgeräumt würde.

Der Gesetzgebungsprozeß ist allerdings derzeit ins Stocken geraten. Ob und ggf. wann solche Vorschläge tatsächlich umgesetzt werden, läßt sich daher im Augenblick nicht sagen. Es bleibt deshalb abzuwarten, ob sich der Gesetzgeber letztendlich im Sinne der Familienforscher für eine erleichterte Einsichtnahme in bzw. Auskunftserteilung aus Personenstandsbüchern entscheiden wird.

8.18 Bekanntgabe des Namens einer Anzeigerstatterin durch die Behörde an den Angezeigten

Einem Landratsamt waren durch eine Eingabe Mängel in einer Einrichtung bekannt geworden. Anlässlich der Überprüfung dieser Einrichtung durch das Landratsamt wollte der Betreiber den Namen der Eingabeführerin wissen. Das Landratsamt kam diesem Wunsch nach und teilte ihm den Namen mit. Der Betreiber der Einrichtung hat daraufhin der Beschwerdeführerin, die selbst die Einrichtung genutzt hatte, gekündigt.

Das Landratsamt meinte, die Bekanntgabe des Namens der Petentin sei zulässig gewesen, da der Betreiber als Beteiligter eines Verwaltungsverfahrens ein Recht auf Akteneinsicht gehabt habe. Diese Auffassung war jedoch aus folgenden Gründen unzutreffend:

Zwar war Art. 29 BayVwVfG (Akteneinsicht durch Beteiligte) im vorliegenden Fall anwendbar, weil die Bekanntgabe des Namens der Anzeigerstatterin nicht zum Zwecke der Sachverhaltsermittlung erfolgt ist ([Art. 2 Abs. 8 BayDSG](#)). Art. 29 BayVwVfG kann als Ausdruck eines allge-

meinen Rechtsgedankens wohl auch analog für behördliche Auskünfte herangezogen werden (vgl. Kopp, VwVfG, § 29 Rdnr. 3 a). Allerdings lagen die Voraussetzungen dieser Vorschrift nicht vor.

Das Recht auf Auskunft aus Akten besteht insoweit, als deren Kenntnis zur Geltendmachung oder Verteidigung der **rechtlichen** Interessen eines Beteiligten erforderlich ist (Art. 29 Abs. 1 Satz 1 BayVwVfG analog). Dies war hinsichtlich des Namens der Anzeigerstatterin für das laufende bau- bzw. wasserrechtliche Verwaltungsverfahren nicht der Fall, da es dem Betreiber der Einrichtung ohne Kenntnis des Namens der Anzeigerstatterin möglich war, sich gegen die Maßnahmen des Landratsamtes zu wehren. Ein rechtliches Interesse an der Bekanntgabe des Namens der Beschwerdeführerin hätte aber z.B. dann bestanden, wenn sie gegenüber dem Landratsamt bewußt wahrheitswidrige Angaben gemacht hätte, um den Betreiber der Einrichtung zu schädigen, und er sich hiergegen hätte zur Wehr setzen wollen. Dafür lagen im vorliegenden Fall jedoch keine Anhaltspunkte vor. Es fehlte schon an einem entsprechenden Vortrag des Betreibers gegenüber den Bediensteten des Landratsamtes. Die Anzeige der Petentin war auch berechtigt, da das Landratsamt aufgrund ihrer Beschwerde Maßnahmen ergriffen hat. Aus Art. 29 Abs. 1 BayVwVfG ergab sich danach kein Recht des Betreibers der Einrichtung auf Nennung des Namens der Anzeigerstatterin durch das Landratsamt.

Diese hatte vielmehr ein schutzwürdiges Interesse an der Geheimhaltung ihres Namens durch das Landratsamt. Dem Bürger, der eine Behörde auf tatsächliche oder vermeintliche Mißstände und Verstöße gegen Rechtsvorschriften hinweist, sollen dadurch keine Nachteile entstehen. Dies ist auch im Interesse von Behörden, die zur ordnungsgemäßen Erfüllung ihrer Aufgaben auf derartige Informationen angewiesen sind. Der Informant ist nur dann nicht schutzwürdig, wenn es sich um haltlose, grob unwahre oder gar verleumderische Angaben handelt. Die Weitergabe des Namens des Informanten an den Angezeigten ist in diesem Fall zulässig, wenn sich dieser mit erlaubten Mitteln gegen derartige Angaben zur Wehr setzen will. Die unzulässige Nennung des Namens der Anzeigerstatterin durch das Landratsamt habe ich beanstandet.

8.19 Unzulässige Datenweitergabe in einem Widerspruchsverfahren

Ein Petent hatte als Nachbar gegen den Bescheid eines Landratsamtes, mit dem dem Betreiber einer angrenzenden Gaststätte die Erlaubnis zum Betrieb eines Wirtschaftsgartens erteilt worden

ist, Widerspruch eingelegt. Im Rahmen des Widerspruchsverfahrens hat das Landratsamt in seinem Vorlagebericht an die Regierung wörtlich ausgeführt: "Als er (Name des Petenten) dann in finanzielle Schwierigkeiten geriet, mußte er das gesamte Anwesen einschließlich Gaststätte an den Kreditgeber bei dem er angeblich sehr hoch verschuldet war, verkaufen." Der Petent, der im Rahmen einer Akteneinsicht Kenntnis von dem Vorlagebericht erhielt, wandte sich gegen diese Behauptung. Er sei weder "sehr hoch verschuldet" gewesen, noch habe er bei der als Kreditgeber genannten Person jemals Schulden gehabt.

Das Landratsamt teilte dazu mit, die vom Petenten angegriffene Aussage beruhe auf einer Information des Sachbearbeiters des Landratsamtes durch einen Mitarbeiter der Gemeindeverwaltung der Wohnortgemeinde des Petenten. Von dort sei auch geäußert worden, die hohe Verschuldung des Petenten sei in seinem Wohnort allgemein bekannt gewesen. Die Regierung erwarte von den Ausgangsbehörden, daß in einem Vorlagebericht nicht nur der Sachverhalt sowie die entscheidenden rechtlichen Erwägungen im Zusammenhang mit dem Erlaß des angegriffenen Verwaltungsaktes dargestellt werden, sondern, daß auch die Hintergründe eines Widerspruchsverfahrens, selbst wenn sie nicht von rechtlicher Bedeutung sind, geschildert werden. Der Regierung soll es damit ermöglicht werden, die Erfolgsaussichten einer eventuellen Rücknahme des Widerspruches würdigen zu können.

Die Weitergabe der gerügten Aussage durch das Landratsamt an die Regierung war eine Übermittlung personenbezogener Daten an eine andere öffentliche Stelle. Mangels einer bereichsspezifischen Regelung beurteilte sich die Zulässigkeit der Datenübermittlung nach [Art. 18 Abs. 1 BayDSG](#). Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist danach zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgabe erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach [Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG](#) zulässig wäre. Erforderlich ist eine Datenübermittlung dann, wenn die Datenkenntnis des Empfängers zur Erreichung des Zwecks der Übermittlung, d.h. zur Erfüllung der Aufgaben des Absenders oder des Empfängers, objektiv geeignet ist und im Verhältnis zu diesem Zweck (d.h. der Aufgabenerfüllung) auch angemessen erscheint (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rdnr. 9). Die datenschutzrechtliche Überprüfung hat ergeben, daß die Datenübermittlung ungeeignet und auch unangemessen und damit unzulässig war.

Im Widerspruchsverfahren ist die Weitergabe personenbezogener Daten von der Ausgangsbe-

hörde an die Widerspruchsbehörde zur Aufgabenerfüllung geeignet, wenn sie zur Sach- oder einer Verfahrensentscheidung durch die Widerspruchsbehörde beitragen kann.

Die Regierung hatte im vorliegenden Fall über den Nachbarwiderspruch des Petenten gegen die gaststättenrechtliche Erlaubnis für den Betrieb eines Wirtschaftsgartens zu entscheiden. Für die Beurteilung der Rechtmäßigkeit des erlassenen Verwaltungsaktes war die finanzielle Situation des Widerspruchsführers ersichtlich irrelevant und konnte die Datenübermittlung daher nicht rechtfertigen.

Jedenfalls nicht von vornherein auszuschließen ist hingegen, daß finanzielle Probleme eines Widerspruchsführers im Hinblick auf eine mögliche einvernehmliche Regelung der Angelegenheit eine Rolle spielen können. Der Ausgangsbehörde ist es deshalb nicht verwehrt, entsprechende Informationen in ihr Verfahren einzubeziehen. Das Landratsamt mußte daher im vorliegenden Fall die Information über die kritisierte Aussage nicht im vornherein berücksichtigt lassen. Es hätte jedoch folgendes in seine Überlegungen einbeziehen und entsprechend verfahren müssen: Die Aussage, der Petent habe, als er in finanzielle Schwierigkeiten geriet, das gesamte Anwesen einschließlich Gaststätte an den Kreditgeber, bei dem er angeblich bereits sehr hoch verschuldet gewesen sei, verkaufen müssen, berührt das allgemeine Persönlichkeitsrecht des Betroffenen in erheblicher Weise. Das Landratsamt hätte diese Behauptung nicht ohne Anhörung des Betroffenen übernehmen, aktenkundig und an die Regierung weitergeben dürfen. Angesichts der Schwere des Vorwurfs und den damit für den Petenten verbundenen möglichen Nachteilen sowie im Hinblick auf den Grundsatz der vorrangigen Datenerhebung beim Betroffenen hätte dem Petenten die Aussage, nachdem das Landratsamt sie für verfahrenserheblich erachtet hatte, mitgeteilt werden müssen und ihm Gelegenheit zur Stellungnahme gegeben werden müssen. Der Petent hätte dann bereits im Abhilfeverfahren seine nachhaltigen Einwendungen gegen die kritisierte Aussage vorbringen können und dabei auch deutlich machen können, daß eine einvernehmliche Regelung im Hinblick auf die Aussage ausgeschlossen ist. Die unzulässige Datenweitergabe habe ich beanstandet.

8.20 Mitteilung über genehmigte Bauvorhaben an die Arbeitsverwaltung zur Bekämpfung der illegalen Beschäftigung und des Leistungsmißbrauchs auf Baustellen

Von Landratsämtern bin ich gefragt worden, ob sie der Arbeitsverwaltung (Sonderprüfgruppen Außendienst Bau) auf Anfrage genehmigte Bauvorhaben mitteilen dürfen. Die Arbeitsverwaltung habe erklärt, sie benötige die Daten zur Bekämpfung der illegalen Beschäftigung und des Leistungsmißbrauchs auf Baustellen. Mit dem Innenministerium vertrete ich dazu folgende Auffassung:

Mangels bereichsspezifischer Regelungen ist die Übermittlung von Daten aus dem Baugenehmigungsverfahren an die Sonderprüfgruppen Außendienst der Arbeitsämter nach [Art. 18](#) des Bayerischen Datenschutzgesetzes zu beurteilen. Danach ist die Übermittlung zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der empfangenden Stelle liegenden Aufgaben erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach [Art. 17 Abs. 1 Nr. 2, Abs. 2-4 BayDSG](#) zulässig wäre ([Art. 18 Abs. 1 BayDSG](#)). Als Zulässigkeitstatbestände für eine Zweckänderung kommen insbesondere [Art. 17 Abs. 2 Nrn. 9 und 10](#) in Betracht: Die Bekämpfung der illegalen Beschäftigung und des Leistungsmißbrauchs sowie die Kontrolle der Werkvertragsvereinbarungen insbesondere mit den mittel- und osteuropäischen Staaten dient der Abwehr erheblicher Nachteile für das Gemeinwohl, da damit das Funktionieren unseres Sozialversicherungssystems sichergestellt werden soll. Auch stellt die illegale Beschäftigung und der Leistungsmißbrauch eine Straftat bzw. eine Ordnungswidrigkeit dar.

Den Arbeitsämtern dürfen für diesen Zweck aber nur solche Daten übermittelt werden, die zu ihrer Aufgabenerfüllung erforderlich sind. Die Übermittlung aller Bauvorhaben ist nicht notwendig. Nach Feststellung des fachlich zuständigen Innenministeriums ist es vielmehr ausreichend, Bauvorhaben mit einer geschätzten Bausumme ab 300 000 DM den Arbeitsämtern für diesen Zweck auf Antrag mitzuteilen.

8.21 Datenschutz in Umlegungsverfahren

Ein Petent wandte sich an mich, nachdem sein Nachbar, für den zu Lasten des Grundstücks des Petenten ein Wasserableitungsrecht in das Grundbuch eingetragen ist, im Rahmen eines Umlegungsverfahrens einen Auszug aus dem Umlegungsplan erhalten hatte, aus dem u.a. hervorgeht, daß der Petent ein Staatsdienerdarlehen erhalten hat und eine Grundschuld auf das Grundstück

eingetragen ist. Ich habe dem Eingabeführer mitgeteilt, daß dies nicht im Einklang mit § 70 Abs. 1 Satz 1 des Baugesetzbuches (BauGB) steht. Danach ist den Beteiligten, zu denen auch Inhaber beschränkt dinglicher Rechte gehören (vgl. § 48 Abs. 1 Nr. 2 BauGB), nur ein **ihre Rechte** betreffender Auszug aus dem Umlegungsplan zuzustellen. Der Nachbar hätte daher den Auszug aus dem Umlegungsplan nur insoweit erhalten dürfen, als sein Wasserableitungsrecht davon berührt war. Die übrigen Daten (z.B. Staatsdienerdarlehen, Grundschuld) wären daher zu schwärzen gewesen.

Ich habe inzwischen die Oberste Baubehörde im Bayerischen Staatsministerium des Innern gebeten, die für die Durchführung von Umlegungsverfahren zuständigen Behörden in geeigneter Form auf die datenschutzrechtliche Problematik des § 70 Abs. 1 Satz 1 BauGB hinzuweisen.

9. Einwohnermeldewesen

9.1 Weitergabe von Meldedaten an Adreßbuchverlage und Parteien

1. Melderegisterauskünfte zur Wahlwerbung

Vor Wahlen häufen sich die Beschwerden von Bürgern über persönlich an sie adressierte Wahlwerbung. Viele Bürger sind mit der Weitergabe ihrer Namen und Anschriften an politische Parteien zu Wahlwerbezwecken nicht einverstanden. Ihnen ist aber offenbar nicht hinreichend bekannt, daß sie nach Art. 35 Abs. 1 Satz 3 des Bayerischen Meldegesetzes (MeldeG) einer Weitergabe ihrer Daten an Parteien und Wählergruppen zu Wahlwerbezwecken durch einfache Mitteilung an ihr Meldeamt widersprechen können. Die bestehende Hinweispflicht bei der Anmeldung (Art. 35 Abs. 1 Satz 4 MeldeG) ist m.E. offensichtlich nicht effektiv. Ich habe deshalb anläßlich der Bundes- und Landtagswahl im Herbst dieses Jahres die Bürger frühzeitig im März mit einer Presseerklärung auf ihr Widerspruchsrecht aufmerksam gemacht.

Nach Art. 35 Abs. 1 Satz 1 MeldeG darf die Meldebehörde Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen in den sechs Monaten vor der Stimmabgabe Auskunft aus dem Melderegister über Vor- und Familiennamen, den Doktorgrad und Anschriften von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen maßgebend ist, es sei denn, der Bür-

ger hat dieser Weitergabe seiner Daten widersprochen.

Zu Fragen im Zusammenhang mit Melderegisterauskünften an politische Parteien zur Wahlwerbung habe ich mich wiederholt in meinen Tätigkeitsberichten geäußert, zuletzt im 17. Tätigkeitsbericht unter [Nr. 9.1](#).

2. Melderegisterauskünfte an Adreßbuchverlage

Nach Art. 35 Abs. 3 Satz 2 MeldeG können die Bürger in Bayern einer Weitergabe ihrer Meldedaten (Vor- und Familiennamen, Doktorgrad und Anschriften) an Adreßbuchverlage widersprechen. Im Saarland hat der Gesetzgeber inzwischen eine Änderung zum dortigen Meldegesetz verabschiedet, nach der die dort bislang wie in den meisten deutschen Ländern bestehende "Widerspruchslösung" durch eine - nach Publikationsmedien differenzierende - "Einwilligungslösung" ersetzt wird. Eine Weitergabe von Meldedaten an Adreßbuchverlage ist danach im Saarland künftig nur noch dann zulässig, wenn der Betroffene hierzu sein Einverständnis erteilt hat. Dabei kann der Betroffene bestimmen, ob die Eintragung in gedruckten, elektronischen oder beiden Verzeichnissen erfolgt. Auch in Nordrhein-Westfalen ist die Zulässigkeit einer Datenübermittlung der Meldebehörden an Adreßbuchverlage ab dem 1. Januar 1999 von einer zuvor erteilten, schriftlichen Einwilligung der Betroffenen abhängig. Vor- und Familiennamen, Doktorgrad und Anschriften dürfen danach nur in gedruckten Adreßbüchern veröffentlicht und nicht mit anderen personenbezogenen Daten verknüpft werden.

3. Einwilligungsregelung als datenschutzfreundliche Lösung

Die "Einwilligungslösungen" in Nordrhein-Westfalen und im Saarland tragen dem Recht der Bürger auf informationelle Selbstbestimmung besser als eine "Widerspruchslösung" Rechnung. Dies gilt in gleicher Weise auch für die Übermittlung von Meldedaten an politische Parteien zur Wahlwerbung. Ich rege daher für die nächste Novellierung des Bayerischen Meldegesetzes an, für die Weitergabe von Adressen an Parteien und an Adreßbuchverlage vergleichbare Regelungen wie in Nordrhein-Westfalen und im Saarland zu schaffen.

Mit der Weitergabe von Meldedaten an Adreßbuchverlage und Parteien hat sich auch die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 in Wiesbaden befaßt und in einer Entschlieung den gesetzgebenden Krperschaften empfohlen, knftig die Einwilligungslsung vorzusehen ([Anlage 16](#)).

9.2 Weitergabe von Melderegisterdaten an die Freiwillige Feuerwehr zur Nachwuchswerbung

Die Freiwillige Feuerwehr ist eine Einrichtung, die gem. Art. 57 Abs. 1 GO, Art. 1 Abs. 1 BayFwG Pflichtaufgaben der Gemeinde wahrnimmt. Sie ist Bestandteil der einheitlichen Verwaltungsbehrde der Gemeinde (vgl. Niese in Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 2 Rdnr. 19). Die Weitergabe von Daten aus dem Melderegister an die gemeindliche Einrichtung Freiwillige Feuerwehr zur Nachwuchswerbung beurteilt sich daher nach Art. 31 Abs. 7 Satz 1 i.V.m. Art. 31 Abs. 1 MeldeG (Nutzung von Daten innerhalb der Gemeindeverwaltung). Die Weitergabe von Familiennamen, Vornamen, Anschriften und ggfs. des Geburtsjahres von Personen, die fr den Feuerwehrdienst in Frage kommen, ist danach zulssig, wenn dies zur rechtmigen Erfllung der in der Zustndigkeit der Feuerwehr liegenden Aufgaben erforderlich ist.

Aufgabe der Freiwilligen Feuerwehr als gemeindliche Einrichtung ist der abwehrende Brandschutz und der technische Hilfsdienst (Art. 4 Abs. 1 BayFwG). Die Datenweitergabe an die gemeindliche Einrichtung Freiwillige Feuerwehr ist erforderlich, wenn sie zur Erfllung dieser Aufgabe objektiv geeignet ist und im Verhltnis dazu auch angemessen erscheint.

Die Weitergabe von Adredaten zur gezielten Werbung von Feuerwehrynachwuchsleuten ist geeignet, die Funktionsfhigkeit der gemeindlichen Einrichtung Freiwillige Feuerwehr durch Bereitstellung einer ausreichenden Anzahl von Feuerwehrdienstleistenden aufrechtzuerhalten. Die Datenweitergabe ist dann angemessen, wenn sich nicht gengend Bewerber melden, um die erforderliche Mindestmitgliederstrke zu erreichen, denn an der Erfllung der in Art. 4 Abs. 1 BayFwG genannten Aufgaben besteht ein erhebliches ffentliches Interesse.

Die Weitergabe von Adredaten aus dem Melderegister an die gemeindliche Einrichtung Freiwillige Feuerwehr ist daher unter dieser Voraussetzung nach Art. 31 Abs. 7 Satz 1 i.V.m. Art. 31 Abs. 1 MeldeG zulssig.

9.3 Automatisierter Datenabgleich einer Stelle für kommunale Verkehrsüberwachung mit dem Einwohnermelderegister

Durch die Eingabe eines Bürgers wurde mir bekannt, daß die kommunale Verkehrsüberwachung einer Stadt vor Versendung eines Anhörbogens oder eines Bußgeldbescheides wegen einer Verkehrsordnungswidrigkeit generell einen Abgleich mit dem Einwohnermelderegister vornimmt, sofern der Halter nach Auskunft der Kfz-Zulassungsstelle im Stadtgebiet wohnt. Die Stadt möchte auf diese Weise feststellen, ob die im örtlichen Fahrzeugregister eingetragene Adresse noch richtig ist. Sie gab an, dies sei notwendig, da bei einem Wohnungswechsel häufig die Ummeldung des Fahrzeuges vergessen werde. Als Abfragekriterien wurden allerdings lediglich der Nachname und das Geburtsdatum des Fahrzeughalters herangezogen.

Ich habe der Stadt mitgeteilt, daß ich gegen den Datenabgleich grundsätzlich keine Bedenken hätte. Das Abfrageverfahren müßte allerdings so ausgestaltet sein, daß die für die Verkehrsüberwachung zuständige Stelle gem. Art. 31 Abs. 7 i.V.m. Abs. 1 des Bayerischen Meldegesetzes (MeldeG) vom Meldeamt nur die Daten erhalte, die zu ihrer Aufgabenerfüllung im konkreten Fall erforderlich seien. Dies sei bei einem Datenabgleich, bei dem sich der Suchbegriff auf den Nachnamen und das Geburtsdatum des Fahrzeughalters beschränke, nicht gewährleistet, da es insbesondere bei häufig vorkommenden Nachnamen nicht ausgeschlossen sei, daß dem Sachbearbeiter in der kommunalen Verkehrsüberwachung auch die Anschriften von Einwohnern mit anderen Vornamen als dem der gesuchten Person mitgeteilt werden. Das kann dazu führen, daß aufgrund einer Personenverwechslung statt des Fahrzeughalters eine an dem Verkehrsverstoß unbeteiligte Person wegen einer vermeintlich von ihr begangenen Verkehrsordnungswidrigkeit angehört wird und im Extremfall, wie der Eingabeführer, sogar mit einem Bußgeld belegt wird. Die Stadt hat das Abfrageverfahren inzwischen geändert. Die Überprüfung der Halteranschrift kann jetzt nur noch anhand der Eingabe des Familiennamens, des Geburtsdatums sowie zusätzlich des Vornamens und des Geschlechtes erfolgen. Nur wenn eine Person mit genau diesen Merkmalen im Einwohnermelderegister gefunden wird, wird der kommunalen Verkehrsüberwachung die Adresse zur Verfügung gestellt. Meiner Anregung wurde damit entsprochen.

10. Ausländerwesen

10.1 Weitergabe personenbezogener Daten vom Ausländeramt an das Arbeitsamt zur Bekämpfung von Leistungsmißbrauch

Ein Ausländeramt erhielt im Rahmen einer sog. Bonitätsprüfung nach § 84 Abs. 1 AuslG davon Kenntnis, daß der Verpflichtungserklärende einerseits Arbeitslosenhilfe erhält, andererseits jedoch lt. einem vorgelegten Kontoauszug über ein beträchtliches Vermögen verfügt. Das Ausländeramt hegte den Verdacht, der Verpflichtungserklärende habe sein Vermögen bei der Beantragung der Arbeitslosenhilfe verschwiegen. Es war nun die Frage zu klären, ob das Ausländeramt dem Arbeitsamt seine Erkenntnis mitteilen darf. Ich vertrete dazu die folgende Auffassung:

Die Information an das Arbeitsamt über Vermögensverhältnisse des Unterzeichners einer Verpflichtungserklärung nach § 84 Abs. 1 AuslG stellt eine Datenübermittlung an eine öffentliche Stelle dar, die einer Rechtsgrundlage bedarf. § 79 AuslG, der generell die Datenübermittlung durch die Ausländerbehörden an das Arbeitsamt regelt, kommt jedoch im vorliegenden Fall nicht in Betracht, da er nur auf die Weitergabe von Daten der unter das Ausländergesetz fallenden Ausländer anwendbar ist (vgl. §§ 1 und 2 AuslG).

Mangels einer bereichsspezifischen Übermittlungsvorschrift richtet sich die Weitergabe der Daten nach [Art. 18 Abs. 1](#) i.V.m. [Art. 17 BayDSG](#). Danach muß die Datenübermittlung zur Erfüllung der in der Zuständigkeit der Ausländerbehörde bzw. des Arbeitsamtes liegenden Aufgaben erforderlich sein und für Zwecke erfolgen, für die eine Nutzung nach [Art.17 Abs. 1 Nr. 2, Abs. 2 - 4 BayDSG](#) zulässig wäre.

Die Datenübermittlung ist erforderlich, wenn das Arbeitsamt die Angaben benötigt, um über die Rücknahme bzw. den Widerruf des Bescheides über Arbeitslosenhilfe, ggf. über die Rückforderung zu Unrecht bezogener Leistungen oder andere geeignete Maßnahmen entscheiden zu können. Dies ist in erster Linie dann der Fall, wenn sicher feststeht, daß tatsächlich ein Leistungsmißbrauch vorliegt.

Man wird aber wohl auch dann die Übermittlung als erforderlich ansehen müssen, wenn zumindest mit hinreichender Wahrscheinlichkeit davon ausgegangen werden kann, daß ein unrechtmäßiger Bezug von Arbeitslosenhilfe gegeben ist und dadurch ein nicht unerheblicher Schaden verursacht wird. Die Aufgabenerfüllung besteht nämlich nicht nur in der Rücknahme, dem Widerruf

etc. an sich, sondern sie umfaßt auch die Prüfung, ob die Voraussetzungen hierfür überhaupt vorliegen. Diese kann vom Arbeitsamt aber nur dann vorgenommen werden, wenn es aufgrund der Datenübermittlung durch das Ausländeramt und daran anknüpfend durch weitere eigene Ermittlungen im Besitz der dazu notwendigen Informationen ist.

Falls das Ausländeramt nicht in der Lage sein sollte, aus eigener Sachkenntnis zu beurteilen, ob die Übermittlung zur Aufgabenerfüllung des Arbeitsamts erforderlich ist, sollte es zuerst beim Arbeitsamt den Fall in anonymisierter Form vortragen und anfragen, ob die Existenz eines Barvermögens in der im Kontoauszug angegebenen Höhe rechtlich für die Gewährung von Arbeitslosenhilfe relevant ist. Sofern das Arbeitsamt die Relevanz bejaht, ist eine Information des Arbeitsamts für seine Aufgabenerfüllung erforderlich.

Im Hinblick auf den Grundsatz der Ersterhebung beim Betroffenen ([Art. 16 Abs. 2 Satz 1 BayDSG](#)) hat sich die Datenübermittlung auf die dafür erforderlichen Angaben zu beschränken, d.h. es dürften zunächst nur die für die Einleitung einer Überprüfung durch das Arbeitsamt notwendigen Daten übermittelt werden.

Da die Übermittlung von Vermögensverhältnissen des Betroffenen mit einer Zweckänderung verbunden ist, muß zudem eine Ausnahme vom Zweckbindungsgrundsatz gegeben sein. Hier kommt zum einen [Art. 17 Abs. 2 Nr. 5 BayDSG](#) in Betracht, der eine Zweckänderung erlaubt, wenn Angaben des Betroffenen überprüft werden sollen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen. Davon ist dann auszugehen, wenn das Arbeitsamt bestätigt, daß bei der Höhe des Vermögens Arbeitslosengeld nicht gewährt wird. Die Zweckänderung könnte allerdings auch auf [Art. 17 Abs. 2 Nr. 6 BayDSG](#) gestützt werden, da Angaben des Betroffenen (zu seinem Vermögen) zur Erlangung von finanziellen Leistungen öffentlicher Stellen (Arbeitslosenhilfe) mit anderen derartigen Angaben verglichen werden sollen.

11. Steuerverwaltung

11.1 ePost in der Steuerverwaltung

In meinem 17. Tätigkeitsbericht ([11.2](#)) habe ich zur Problematik der Verarbeitung von Steuerdaten durch private Dritte Stellung genommen.

Ausgangspunkt der Überlegungen war die sich verstärkende Praxis von Kommunen gewesen, die Kuvertierung und den Versand von Lohnsteuerkarten auf private Mailing-Service-Firmen zu übertragen.

Auch im Berichtszeitraum ist dieser Trend ungebrochen.

Neue Überlegungen waren veranlaßt, als die Frage an mich herangetragen wurde, ob der Druck und Versand von Lohnsteuerkarten mit Hilfe des ePost-Verfahrens zulässig sei.

Bei diesem Verfahren ist es möglich, zeichencodierte Nachrichten für beliebige Empfänger jederzeit elektronisch bei der zuständigen ePost-Station einzuliefern. Die elektronischen Informationen werden an die empfängernächste ePost-Station weiterübermittelt und dort in körperliche Nachrichten umgewandelt, die mit einem Logo, mit Grafik, Unterschriftenfaksimiles usw. versehen werden können. Die Ausdrücke werden entsprechend dem Wunsch des Kunden als Briefe oder Infopost an den Empfänger ausgeliefert.

In dem von mir zu beurteilenden Sachverhalt war an die Zwischenschaltung eines zertifizierten Vertriebspartners der Deutschen Post AG gedacht, der die von den Kommunen übermittelten (Lohnsteuer-)Daten in ein bestimmtes Druckformat konvertiert und an die nächste ePost-Station weiterleitet.

Im Einvernehmen mit dem Staatsministerium der Finanzen vertrete ich folgende Rechtsauffassung:

Aufgrund der Bestimmung des § 30 Abs. 1 AO sind Amtsträger oder diesen gleichgestellte Personen verpflichtet, das Steuergeheimnis zu wahren. Die Finanzverwaltung - und damit auch die bei der Aufstellung von Lohnsteuerkarten als örtliche Finanzbehörde handelnden Kommunen (§ 39 Abs. 6 EStG) - muß die Wahrung des Steuergeheimnisses nicht nur rein rechtlich, sondern auch faktisch sicherstellen. Dies ist beim ePost-Verfahren nicht gewährleistet. Die Finanzverwaltung verliert vielmehr die Herrschaft über die von ihr gelieferten Daten. Sie kann bspw. nicht sicherstellen, daß die im ePost-Verfahren eingesetzten Personen nicht unbefugt die gelieferten Daten speichern. Das ePost-Verfahren birgt auch die zumindest theoretische Möglichkeit in sich,

daß außerhalb der Finanzverwaltung ein umfangreicher Gesamtdatenbestand der Arbeitnehmer mit deren für den Lohnsteuerabzug relevanten Werten entsteht. Zu berücksichtigen waren auch wettbewerbsrechtliche Aspekte. Bei einer Vergabe von derartigen Aufträgen an die Deutsche Post AG ist nicht auszuschließen, daß entsprechende Aufträge künftig auch an andere Telekommunikationsunternehmen, welche nicht der Kontrolle durch deutsche Behörden und Gerichte unterliegen, vergeben werden müßten.

Mit dem Staatsministerium der Finanzen sehe ich mich einig, daß eine Nutzung des ePost-Verfahrens bei der Vergabe von Aufgaben der Steuerverwaltung an private Dritte mit § 30 Abs. 1 AO nicht vereinbar ist.

Dieses Beispiel zeigt erneut, daß meine Forderung nach einem Zulässigkeitsrahmen von Outsourcing-Maßnahmen im Bereich der Steuerverwaltung unverändert aktuell ist. Dies wäre bspw. im Rahmen der Neuaufnahme der Diskussion zu einem AO-Änderungsgesetz möglich.

11.2 Veröffentlichung personenbezogener Daten in den Mitteilungsniederschriften der Steuerberaterkammern München und Nürnberg

Durch mehrere Eingaben wurde ich auf die personenbezogene Veröffentlichungspraxis bei Verurteilungen und strafbewehrten Unterlassungserklärungen in den Mitteilungsschriften der Steuerberaterkammern aufmerksam.

Auf Nachfrage teilten die Kammern mit, daß der Wortlaut der gerichtlichen Entscheidung bzw. Unterlassungserklärung sowie Name und Anschrift der davon betroffenen Person bzw. Vereinigung veröffentlicht werde. Dabei handle es sich in der Regel nicht um Kammerangehörige, sondern um Personen, gegen die die Kammer wegen unerlaubter Hilfe in Steuersachen einschließlich überzogener Werbung rechtlich vorgegangen sei.

Die Kammern wie auch das Staatsministerium der Finanzen verweisen auf § 76 Abs. 1 StBerG als Rechtsgrundlage. Nach dieser Vorschrift hätten die Kammern die Aufgabe, die beruflichen Belange der Gesamtheit der Mitglieder zu wahren und die Erfüllung der beruflichen Pflichten zu überwachen.

Ich sehe in dieser Rechtsvorschrift keine ausreichende Rechtsgrundlage für die augenblickliche Veröffentlichungspraxis.

§ 76 Abs. 1 StBerG beschreibt nur allgemein die Aufgaben der Kammern. Die Vorschrift stellt aber keinesfalls eine Befugnis für die in Rede stehenden Datenübermittlungen dar, da der Schluß von der Aufgabe auf die Befugnis im Gegensatz zur umgekehrten Schlußfolgerung nicht zulässig ist. Hinzuweisen ist auch auf das vom Bundesverfassungsgericht in seiner Entscheidung zum Recht auf informationelle Selbstbestimmung (BVerGE 65, 44) geforderte rechtsstaatliche Gebot der Normenklarheit. Zum zulässigen Umfang des Eingriffs in das genannte Grundrecht sagt § 76 Abs. 1 StBerG als bloße Aufgabenzuweisungsnorm seiner Natur nach verständlicherweise nichts aus.

Weiterhin war zu prüfen, ob Bestimmungen des Bayerischen Datenschutzgesetzes selbst die Veröffentlichungspraxis rechtfertigen können. Durch die Veröffentlichung in den Kammermitteilungen erfolgt eine Datenübermittlung an Personen außerhalb des öffentlichen Bereichs. Die Empfänger der Mitteilungen (die Steuerberater) sind nicht Mitarbeiter der Kammern, sie werden durch die Kammern als Außenstehende verwaltet. Darüber hinaus ist nicht auszuschließen, daß die Kammermitteilungen auch von Personen außerhalb des Kreises der Kammermitglieder gelesen werden. [Art. 19 BayDSG](#) regelt derartige Datenübermittlungen an nicht-öffentliche Stellen. Es wird nicht verkannt, daß die Kammern bei der Ahndung von Wettbewerbsverstößen auf die Mithilfe der Berufsmitglieder angewiesen sind.

Ein Hinweis an die Kammern, daß ein Wettbewerbsverstoß vorliegen könnte, wird aber mit oder ohne Kenntnis eines "Vorverstoßes" erfolgen, denn es ist zu bezweifeln, daß die Kammerangehörigen in der Regel die in Frage stehenden Veröffentlichungen derart archiviert haben, daß ein aktueller Verstoß mit einem ggf. weiter zurückliegenden Verstoß in Zusammenhang gebracht werden könnte. Die Prüfung, ob eine (erneute) Wettbewerbsverletzung bzw. ein Verstoß gegen eine bereits abgegebene Unterlassungserklärung vorliegt, wird in jedem Fall durch die Kammern vorgenommen. Eine personenbezogene Veröffentlichung von Verstößen ist daher nicht erforderlich im Sinne des [Art. 19 Abs. 1 Nr. 1 BayDSG](#).

Die Zulässigkeitsprüfung scheidet aber auch an der bestehenden Zweckbindung:

Unstreitig gehört es aufgrund der Bestimmung des § 76 Abs. 1 StBerG zu den Aufgaben der Kammern, Zuwiderhandlungen gegen das Verbot der unerlaubten Hilfeleistung in Steuersachen und Wettbewerbsverstöße (u.a. überzogene Werbung) im Hinblick auf die Belange der Gesamtheit der Mitglieder abzuwehren.

Für diese Zwecke ist eine Verarbeitung der in Rede stehenden Daten bei den Kammern zulässig.

Für eine Zweckänderung (Datenübermittlung an Dritte) käme wohl nur [Art. 17 Abs. 2 Nr. 9 BayDSG](#) in Betracht. Danach wäre eine Datenübermittlung zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben zulässig, wenn sie "zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist."

Eine geordnete Steuerrechtspflege ist durchaus als wichtiges Gemeinschaftsgut anzusehen. Für Zweckänderungen nach [Art. 17 Abs. 2 Nr. 9 BayDSG](#) reicht allerdings die Abwehr von bloßen Nachteilen für das Gemeinwohl nicht aus. Der abzuwehrende Nachteil muß vielmehr "erheblich" sein. Dies bedingt nach dem Rechtsempfinden der Allgemeinheit das Vorliegen wesentlicher Nachteile für das Gemeinwohl. Diese Voraussetzungen liegen nicht vor. Die flächendeckende Verbreitung der Daten ist zur Abwehr nicht erforderlich.

Auch [Art. 19 Abs. 1 Nr. 2 BayDSG](#) kann nicht als Rechtsgrundlage für die Veröffentlichung dienen. Aufgrund der beschränkten Konkurrenzsituation vermag ich ein berechtigtes Interesse an der Datenübermittlung allenfalls in der Person des den (Wettbewerbs-)Verstoß anzeigenden Kammermitglieds zu sehen und u.U. der Kammermitglieder in einem regional eng begrenzten Umkreis zum Sitz des Wettbewerbsverletzers, keinesfalls jedoch in der Gesamtheit der Kammermitglieder und auch nicht näher quantifizierbarer außenstehender Dritter.

Aus obigen Ausführungen ergibt sich, daß die augenblickliche Veröffentlichungspraxis keine gesetzliche Grundlage hat. Ich habe deshalb eine formelle Beanstandung gem. [Art. 31 Abs. 1 BayDSG](#) ausgesprochen und die Kammern zur Einstellung des bisherigen Verfahrens aufgefordert. Die Steuerberaterkammer Nürnberg hat inzwischen mitgeteilt, daß sie von einer Veröffentlichung vorerst absehen wird. Eine entgeltliche Gegenäußerung der Kammern steht aber noch aus.

11.3 Führung von Fahrtenbüchern für steuerliche Zwecke durch Ärzte

Durch das Jahressteuergesetz 1996 wurde die ertragssteuerliche Behandlung der Nutzung betrieblicher Kraftfahrzeuge für Privatfahrten geändert. Der private Nutzungsanteil ist danach monatlich mit 1 v.H. des inländischen Listenpreises anzusetzen. Abweichend davon kann ein Steuerpflichtiger auch die tatsächlichen Kosten für Privatfahrten der Besteuerung zugrunde legen,

wenn er das Verhältnis der privaten zu den übrigen Fahrten durch ein ordnungsgemäßes Fahrtenbuch nachweist. Ein ordnungsgemäßes Fahrtenbuch muß nach den bestehenden Einkommensteuer- bzw. Lohnsteuer-Richtlinien mindestens die Angabe des Datums, des Kilometerstands zu Beginn und am Ende der einzelnen Auswärtstätigkeit sowie Angaben zu Reiseziel, -route und -zweck enthalten.

Die Finanzverwaltung hat es bisher für ausreichend erachtet, daß Ärzte als Reisezweck die Angabe "Patientenbesuch" neben den übrigen erwähnten Merkmalen im Fahrtenbuch aufführen. Mit Wirkung vom 1.1.1998 hat das Bundesministerium der Finanzen in einem Schreiben an die Bundesärztekammer nunmehr mitgeteilt, daß ein ordnungsgemäßes (und damit steuerlich anzuerkennendes) Fahrtenbuch bei Ärzten nur vorliegt, wenn als Reisezweck Name und Anschrift des besuchten Patienten angegeben werde.

Gegen diese Anordnung haben sich u.a. mehrere Landesärztekammern gewandt. Auch ich wurde um Stellungnahme gebeten.

Die Landesärztekammern sehen in dem Verlangen zur Angabe des Patientennamens einen Verstoß gegen die ärztliche Schweigepflicht i.S. § 203 Abs. 1 StGB und einen Verstoß gegen das u.a. der Berufsgruppe der Ärzte eingeräumte steuerliche Auskunftsverweigerungsrecht nach § 102 Abs. 1 Nr. 3 c Abgabenordnung (AO). § 102 Abs. 1 Nr. 3 c AO bestimmt, daß die Auskunft verweigern können, "... Ärzte, über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist."

Zu diesem Spannungsverhältnis zwischen ärztlicher Schweigepflicht einerseits und steuerlichen Belangen andererseits habe ich eine Stellungnahme des Staatsministeriums der Finanzen eingeholt. Das Staatsministerium der Finanzen hat auf ein Schreiben des Bundesministeriums der Finanzen verwiesen. Dieses vertritt darin die Auffassung, daß für die Entscheidung der Frage, ob ein Arzt die Angabe des Namens des Patienten im Fahrtenbuch verweigern könne, es allein auf die Auslegung des § 102 Abs. 1 Nr. 3 c AO ankomme. In den Nrn. 2 und 4 des § 102 Abs. 1 AO habe der Gesetzgeber ausdrücklich bestimmt, daß die Auskunft auch "über die Personen" verweigert werden könne. In den Nrn. 1 und 3 des § 102 Abs. 1 AO fehle dagegen eine solche Regelung. Daraus folge, daß sich das Auskunftsverweigerungsrecht der in § 102 Abs. 1 Nr. 3 AO genannten Berufsgruppen nicht auf Namen und Anschriften ihrer Kunden, Patienten oder Mandanten erstrecke. Im übrigen sei die eingangs erwähnte Pauschalbesteuerung der Regelfall. Der Arzt könne also bei Anwendung der Pauschalierung eine Bekanntgabe des Patientennamens

vermeiden. Der Arzt sei darüber hinaus nicht gehindert, von seinen Patienten eine ausdrückliche Einwilligung zur Aufnahme ihrer Namen in ein Fahrtenbuch zu erbitten.

Ich vermag aus folgenden Gründen diese Auffassung nicht zu teilen:

Die erwähnte Pauschalregelung kann unter bestimmten Voraussetzungen zu einer unangemessenen Besteuerung führen. Zur Vermeidung eines steuerlichen Nachteils ist der betroffene Arzt deshalb gezwungen, ein steuerlich anzuerkennendes Fahrtenbuch zu führen.

Nach § 90 AO ist ein Beteiligter (i.d.R. der Steuerpflichtige) zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Der Steuerpflichtige kommt seiner Mitwirkungspflicht insbesondere dadurch nach, daß er die für die Besteuerung erforderlichen Auskünfte erteilt (§ 93 Abs. 1 AO).

Die erwähnte generelle Auskunftspflicht wird durch die Auskunftsverweigerungsrechte in §§ 101 ff AO (hier § 102 AO: Auskunftsverweigerungsrecht zum Schutz bestimmter Berufsgeheimnisse) allerdings wieder relativiert. Damit wird bei Inanspruchnahme des Auskunftsverweigerungsrechts eine Einschränkung der Sachaufklärung hingenommen.

§ 102 AO ist im wesentlichen Teil wortgleich mit der Bestimmung des § 53 StPO. Zum Umfang des dort geregelten Zeugnisverweigerungsrechtes existiert Rechtsprechung, welche das Zeugnisverweigerungsrecht auch auf Name und Anschrift eines ärztlichen Patienten ausdehnt.

Ich halte die von der Rechtsprechung aufgestellten Kriterien zu § 53 StPO auf § 102 AO für voll übertragbar. Bestärkt in dieser Auffassung werde ich durch ein Schreiben des Bundesministers der Justiz an den Hauptgeschäftsführer des Bundesverbandes der Freien Berufe, in dem festgestellt wird, daß es den Angehörigen der in § 102 Abs. 1 Nr. 3 AO genannten Berufsgruppen aufgrund der ihnen obliegenden Verschwiegenheitspflicht verwehrt ist, ein Fahrtenbuch entsprechend der (geänderten) Auffassung der Finanzverwaltung zu führen. Zum Umfang des Auskunftsverweigerungsrechtes wird festgestellt, daß dieses auch Name und Anschrift der Patienten umfasse.

Die vom Bundesministerium der Finanzen angesprochene Möglichkeit, die Zustimmung des Patienten zur Aufnahme in das steuerliche Fahrtenbuch einzuholen, erscheint mir zur Problemlösung wenig geeignet. Da das Finanzamt, anders als eine private Verrechnungsstelle, mit dem Behandlungsverhältnis Arzt - Patient nichts zu tun hat, dürfte die Einholung der Zustimmung vielfach auf Unverständnis und Ablehnung stoßen. Das Vertrauensverhältnis zwischen Arzt und Patient kann durch ein derartiges Ansinnen belastet werden.

Im Hinblick darauf, daß Ausgangspunkt des geschilderten Sachverhalts eine Anordnung des Bundesministeriums der Finanzen war, habe ich mich auch an den Bundesbeauftragten für den Datenschutz gewandt. Dieser hat das Bundesministerium der Finanzen inzwischen formell gem. [§ 25 Abs. 1 BDSG](#) beanstandet.

Das Staatsministerium hat mir inzwischen mitgeteilt, daß sich die AO-Referenten des Bundes und der Länder mit der Problematik befassen werden.

12. Personalwesen

12.1 Personalakten

Die bereits in meinem letzten Tätigkeitsbericht unter [Nr. 12.1](#) geschilderten Probleme bei der Umsetzung der Regelungen zur Führung von Personalakten nach dem Bayerischen Beamten-gesetz bestehen nach wie vor.

Personalnebenakten

Bei der datenschutzrechtlichen Prüfung verschiedener Behörden (u.a. Amtsgericht, Beamten-fachhochschule) stellte ich fest, daß zum Teil Nebenakten geführt wurden, die inhaltlich dem kompletten Grundakt entsprachen. Dies widerspricht Art. 100 a Abs. 2 Satz 3 Halbsatz 2 Bayer. Beamten-gesetz, wonach Nebenakten nur solche Unterlagen enthalten dürfen, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. Nebenakten sind nach der Gesetzesbegründung nur insoweit zulässig, als sie für die Aufgabenerfüllung "unerläß-lich" sind, was in den mir bekanntgewordenen Fällen nicht der Fall war. Darüber hinaus wurde die vorgeschriebene regelmäßige Aussonderung von Unterlagen über Erholungsurlaub, Erkran-kungen, Umzugs- und Reisekosten nach fünf Jahren nach Ablauf des Bearbeitungsjahres nicht vorgenommen. Um die vorgesehene Aussonderung in der Praxis zu erleichtern, empfiehlt es sich, für diese Unterlagen einen Teilakt anzulegen.

Verzeichnis der Teil- und Nebenakten

Das in den Grundakt aufzunehmende Verzeichnis aller Teil- und Nebenakten fehlt nach meiner Erfahrung häufig. Dieses ist jedoch unbedingt erforderlich, um das Einsichtsrecht des Bedien-steten in seinen vollständigen Personalakt gewährleisten zu können. Die Grundakten führenden Personalstellen sollten hierauf besonders achten.

Aussonderung

Hinsichtlich der Aussonderung abgeschlossener Personalakten (und auch Sachakten) konnte ich bei meinen Prüfungen die Tendenz feststellen, daß die Akten solange aufbewahrt werden, bis die Kapazität der Registraturen erschöpft ist. Eine regelmäßige Aussonderung und Anbietetung abgeschlossener Personalakten an das zuständige staatliche Archiv ist nicht nur gesetzlich vorgesehen, sondern auch aus Platzgründen und zur Entlastung der Registraturen sinnvoll (vgl. Art. 100 g BayBG, Aussonderungsbekanntmachung vom 19.11.1991, AllMBl S. 884). Nach Auskunft der Generaldirektion der staatlichen Archive bestehen keine Aufnahme Probleme bei den staatlichen Archiven.

Wegen der oben erwähnten Umsetzungsschwierigkeiten habe ich das Bayerische Staatsministerium der Finanzen gebeten, ergänzende Richtlinien zu erlassen. Nach Mitteilung des Ministeriums ist vorgesehen, die veralteten, zum Teil im Widerspruch zu geltenden Vorschriften stehenden Verwaltungsvorschriften über die Personalakten vom 01.06.1967 förmlich aufzuheben und bei Bedarf Vollzugshinweise zu geben. Den einzelnen Ressorts bleibe es unbenommen, für den eigenen Geschäftsbereich entsprechende Richtlinien zu erlassen.

12.2 Nutzung von Personaldaten im Rahmen der Budgetierung

Von Kommunen und Krankenhäusern erhalte ich immer wieder Anfragen, ob es im Zuge der Budgetierung zulässig ist, den Budgetverantwortlichen für die Personalkostenplanung und -kontrolle die genauen Gehaltsdaten der einzelnen Mitarbeiter zur Verfügung zu stellen.

Ich vertrete hierzu folgende Auffassung:

Zu den Gehaltsdaten zählen üblicherweise Daten über die Eingruppierung, den Bruttobezug, den Arbeitgeberanteil zur Sozialversicherung und ähnliches. Es handelt sich somit um Personalaktendaten. Bei einer Nutzung dieser Daten sind für Beamte die Bestimmungen zum Umgang mit Personalaktendaten zu beachten. Ich halte diese Bestimmungen auch für Beschäftigte des Tarifbereichs für analog anwendbar. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verwendet werden und nur soweit dies zu Zwecken der Personalverwaltung oder -wirtschaft erforderlich ist.

Die Personalkostenplanung und -kontrolle als Teil der Budgetierung unterfällt dem Begriff "Personalwirtschaft". Weitere Voraussetzung ist die Übertragung entsprechender Kompetenzen auf

die einzelnen leitenden Mitarbeiter. Unabhängig davon ist jedoch zu prüfen, ob die vorgesehene Datenweitergabe (Nutzung) sowohl dem Grunde nach als auch im beabsichtigten Umfang erforderlich ist. Es ist grundsätzlich der geringste Eingriff zu wählen. Auch ein Zugriff über das Personalverwaltungssystem hat sich hieran zu orientieren.

An dieser Erforderlichkeit fehlte es in den bei mir angefragten Fällen: Keine der Stellen konnte bisher ausreichend darlegen, daß eine DM-genaue Einzelfallabrechnung für jeden Beschäftigten zur Kostenplanung sinnvoll und erforderlich ist. Die nicht vorausplanbaren kostenwirksamen Faktoren (Änderung des Familienstandes, Geburt von Kindern, Krankheitszeiten, Umzugskosten usw.), die die Gesamtpersonalkosten beeinflussen, machen eine präzise Schätzung der zu erwartenden Kosten im Einzelfall regelmäßig unmöglich. Der Budgetverantwortliche sollte daher der Verwendung aktueller Durchschnittswerte den Vorzug geben, die in der einschlägigen Fachliteratur veröffentlicht werden.

12.3 Mitarbeiterdaten im Internet

Mit der wachsenden Bereitschaft der Kommunen sich im Internet darzustellen, erreichen mich zunehmend Anfragen, ob Angaben über die Zuständigkeiten von Mitarbeitern der Verwaltung ins Internet eingestellt werden dürfen.

Ich halte die Veröffentlichung von Daten der Behördenbediensteten für zulässig, wenn sie zur ordnungsgemäßen Aufgabenerfüllung der betreffenden Kommune erforderlich ist. Hierunter fällt grundsätzlich auch die Information, welcher Bedienstete der richtige Ansprechpartner für das Anliegen des Bürgers ist. Dies kann jedoch nur für Bedienstete gelten, die Funktionen mit "Außenwirkung" in der Verwaltung wahrnehmen. Dieser Personenkreis muß aufgrund seiner auf die Öffentlichkeit bezogenen Aufgabenstellung daher beispielsweise hinnehmen, daß von ihm Name, Amts- und Dienstbezeichnung, Tätigkeitsbereich und Funktion sowie die dienstliche Anschrift und Telefonnummer veröffentlicht werden.

Eine solche Außenwirkung fehlt meines Erachtens i.d.R. für lediglich innere Dienste, wie z.B. Registratur, Botendienst, zentraler Schreibdienst u.ä. Eine Veröffentlichung der Daten dieses Personenkreises ist nur nach Erteilung einer ausdrücklichen Einwilligung der Betroffenen zulässig.

Allerdings stellt sich die Frage, ob eine breit gestreute Information über Daten der Sachbearbei-

terebene im Internet überhaupt sinnvoll ist; das muß bezweifelt werden:

Die Verbreitung von Daten über das Internet ist eine völlig neue Qualität der Veröffentlichung. Sie erreicht weltweit einen ungleich größeren Personenkreis als jede auflagenbegrenzte schriftliche Veröffentlichung (Beispiel Behördenwegweiser). Zudem schafft die beschriebene Veröffentlichung neue Risiken (kommerzielle Nutzung), die den Beteiligten bewußt sein sollten, da die Einhaltung der Zweckbindung in solchen Verzeichnissen technisch nicht sicherzustellen ist und zudem diese Personendaten mit sonstigen elektronischen Dateien kombiniert werden können (Adreß- und Telefonverzeichnisse).

Zu beachten ist, daß eine Veröffentlichung der Privatanschrift der Bediensteten zum Schutz vor Belästigungen auf jeden Fall unzulässig ist. In einigen Verwaltungsbereichen können auch Sicherheitsbedenken gegen eine Veröffentlichung der genannten Mitarbeiterdaten sprechen

12.4 Fragebogen zur Einstellung von Auszubildenden

Durch Presseartikel erfuhr ich, daß die Städtische Berufsfachschule für Krankenpflege der Landeshauptstadt München in Zusammenarbeit mit einem berufspsychologischen Institut einen Fragebogen zur Bewerberauswahl für Ausbildungsplätze an der Schule verwendete, der aufgrund einzelner Fragen aus dem Intimbereich großes Aufsehen erregte. Er enthielt u.a. detaillierte mit "Ja" oder "Nein" zu beantwortende Fragen zum Familien- (z.B.: "Ich wurde von Vater oder Mutter öfter geschlagen"; "Meine Eltern hatten oft Auseinandersetzungen") und zum Sexualleben (z.B.: "Mir sind sexuelle Handlungen unangenehm; ich versuche sie zu vermeiden"; "Ich kann mich in sexuellen Dingen als guten Partner bezeichnen") der Bewerberinnen und Bewerber. Ich habe die Landeshauptstadt München auf die Rechtswidrigkeit dieser Datenerhebung gem. [Art. 16 Abs. 1 BayDSG](#) hingewiesen. Der Schutz des Persönlichkeitsrechts der Bewerber läßt nur solche Fragen zu, an denen der (zukünftige) Arbeitgeber zur Beurteilung der Eignung und Befähigung ein objektiv berechtigtes Interesse hat. Es ist zwischen Fragen nach dem persönlichen und beruflichen Werdegang und Fragen mit einem direkten Bezug zur Intimsphäre zu unterscheiden. In letzterem Fall ist ein besonderer Schutz geboten. Die hier gebotene Abwägung zwischen dem Interesse der Bewerber an der Wahrung ihrer Privatsphäre und dem (öffentlichen) Interesse an der Ermittlung ihrer Eignung für die Berufsfachschule führt dazu, daß diese detaillierten Fragen zum Familien- und zum Sexualleben unzulässig sind, da sie über das hinausgehen,

was für eine ordnungsgemäße Beurteilung der Eignung der Bewerber erforderlich ist. Gerade Fragen aus dem sexuellen Bereich sind für die Beurteilung einer Eignung zur Krankenpflegeausbildung unverhältnismäßig.

Außerdem wurden durch den Fragebogen personenbezogene Daten durch das berufspsychologische Institut im Auftrag der Landeshauptstadt München ohne schriftlichen Auftrag erhoben, obwohl [Art. 6 Abs. 2 Satz 2 BayDSG](#) eine solche schriftliche Auftragserteilung vorschreibt.

Die Landeshauptstadt München hat den Fragebogen schon bald nach seinem öffentlichen Bekanntwerden zurückgezogen und früher abgelehnten Bewerbern eine nochmalige Bewerbungsmöglichkeit ohne "Intimfragen" eingeräumt. Eine abschließende Stellungnahme war mir noch nicht möglich, da sich die Landeshauptstadt München noch nicht abschließend geäußert hat.

13. Gewerbe und Handwerk

13.1 Verlängerung der Speicherdauer beendeter Berufsausbildungsverhältnisse

Eine Handwerkskammer teilte mir mit, daß die in der Handwerksordnung vorgesehene Speicherdauer von 50 Jahren für beendete Berufsausbildungsverhältnisse zu kurz bemessen sei. Sie erhalte täglich Anfragen der Rentenversicherungsträger zu Ausbildungsverhältnissen bzw. Prüfungen, die länger als 50 Jahre zurücklägen. Da die nach der Beendigung des Berufsausbildungsverhältnisses in einer gesonderten Datei zu speichernden Daten gemäß § 28 Abs. 6 der Handwerksordnung (HandwO) nach spätestens 50 Jahren vernichtet werden müßten, könnten diese Auskünfte nicht mehr erteilt werden, was in vielen Fällen zum Nachteil der Versicherten wäre, sofern sie nicht anderweitig einen Nachweis für die von den Rentenversicherungsträgern geforderten Daten erbringen könnten.

Ich hatte keine datenschutzrechtlichen Bedenken gegen eine solche Verlängerung der Speicherfrist, da sie im Interesse des Betroffenen war. Ich habe mich an das Bayerische Staatsministerium für Wirtschaft, Verkehr und Technologie gewandt, das in der Folge einen Vorschlag zur Verlängerung der Speicherdauer in das Gesetzgebungsverfahren zur Änderung der Handwerksordnung eingebracht hat. Die Gesetzesänderung wurde inzwischen vom Bundestag verabschiedet und trat am 01.04.1998 in Kraft (Zweites Gesetz zur Änderung der Handwerksordnung und anderer handwerksrechtlicher Vorschriften, BGBl. I S. 596 ff.). Die Speicherung beträgt jetzt nach § 28 Abs. 6 Satz 1 HandwO 60 Jahre. Damit kann nun in vielen Fällen, in denen dies früher

nicht möglich war, der für die Rentenversicherung wichtige Nachweis des Berufsausbildungsverhältnisses erbracht werden.

13.2 Gewerbeabmeldung von Amts wegen

Im 17. Tätigkeitsbericht habe ich unter [Nr. 13.1.2](#) darüber berichtet, daß nach der damaligen Rechtslage ein Gewerbetreibender, der einer bestands- bzw. rechtskräftigen Gewerbeuntersagung zuwider gehandelt und sein Gewerbe nicht abgemeldet hatte, gegenüber privaten Dritten ein ordnungsgemäß angemeldetes Gewerbe vortäuschen konnte. Eine Auskunft über das Gewerbeuntersagungsverfahren war nicht möglich, weil § 11 Abs. 5 der Gewerbeordnung (GewO) eine solche Datenübermittlung an private Dritte zur Verfolgung privatrechtlicher Ansprüche nicht zuläßt. Bei einer Auskunft aus der Gewerbeanzeige nach § 14 Abs. 8 GewO wurde wegen der fehlenden Anzeige der Gewerbeabmeldung ein ordnungsgemäß angemeldetes Gewerbe vorgetäuscht. Die Abmeldung des Gewerbes konnte nach der früheren Rechtslage nicht von Amts wegen erfolgen, sondern mußte unter Umständen zeitraubend mit Zwangsmitteln durchgesetzt werden.

Inzwischen hat der Gesetzgeber reagiert und im Zweiten Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 16. Juni 1998, BGBl 1998, Teil I, S. 1291 ff. dem § 14 Abs. 1 GewO folgenden Satz angefügt: "Steht die Aufgabe des Betriebes eindeutig fest und ist die Abmeldung nicht innerhalb eines angemessenen Zeitraums erfolgt, kann die Behörde die Abmeldung von Amts wegen vornehmen."

13.3 Mitteilungen von Gewerbeämtern an Industrie- und Handelskammern über Reisegewerbe

Eine bundesweit durchgeführte Umfrage der IHK Leipzig hat ergeben, daß auch in Bayern Industrie- und Handelskammern von einigen Gewerbeämtern regelmäßig Mitteilungen über erteilte Reisegewerbekarten bzw. die Ausübung einer reisegewerbekartenfreien Tätigkeit erhielten. Für eine solche Datenübermittlung gibt es keine Rechtsgrundlage.

Gem. § 14 Abs. 5 Nr. 1 GewO darf die Gewerbebehörde regelmäßig lediglich die dort genannten Daten der Gewerbeanzeigen des stehenden Gewerbes an die Industrie- und Handelskammer übermitteln. Die Erteilung von Reisegewerbekarten nach § 55 GewO ist hiervon nicht erfaßt.

Ebenfalls unzulässig ist gem. § 55 c GewO die Übermittlung von Daten der reisegewerbekartenfreien Tätigkeiten nach § 55 a GewO, denn in § 55 c GewO ist die Anwendung von § 14 Abs. 5 GewO nicht mit aufgenommen worden. Die fallweise Übermittlung von Einzeldaten gem. § 14 Abs. 6 - 8 und 9 GewO ist nur aus Gewerbeanzeigen nach § 14 und § 55 c GewO vorgesehen, nicht jedoch aus Reisegewerbekarten.

§ 138 Abs. 1 Satz 1 Halbsatz 2 der Abgabenordnung (AO) läßt lediglich eine regelmäßige Unterrichtung des Finanzamtes über den Beginn eines Reisegewerbes durch die Wohnsitzgemeinde des Reisegewerbetreibenden zu.

Damit besteht für eine regelmäßige Übermittlung von Daten über Reisegewerbe an die Industrie- und Handelskammern keine rechtliche Grundlage. Gleiches gilt allgemein für die Datenübermittlung aus der Reisegewerbekarte an öffentliche und nicht-öffentliche Stellen.

Ich habe das Bayerische Staatsministerium für Wirtschaft, Verkehr und Technologie gebeten, die rechtswidrige Verwaltungspraxis der Gewerbeämter zu unterbinden. Das Wirtschaftsministerium hat das Thema inzwischen auf einer Gewerberechtsarbeitstagung erörtert und die Vollzugsbehörden entsprechend unterrichtet.

13.4 Veröffentlichung von Gewerberegisterdaten im Internet

Gemeinden und Landkreise erwägen im Rahmen ihrer Präsentation im Internet oder allgemein zur Förderung der heimischen Wirtschaft teilweise auch die Einstellung der in ihrem Hoheitsgebiet tätigen Unternehmen. Als Datenquelle kommt dabei das Gewerberegister in Betracht. Die Veröffentlichung dieser Daten ist unproblematisch, soweit der Betroffene hierzu seine Einwilligung erteilt hat. Fehlt es jedoch an der ausdrücklichen Zustimmung des Gewerbetreibenden, so ist die Einstellung dieser Daten ins Internet aus folgendem Grund unzulässig:

Nach § 14 Abs. 8 der Gewerbeordnung (GewO) darf einer nicht-öffentlichen Stelle der Name, die betriebliche Anschrift und die angezeigte Tätigkeit eines Gewerbetreibenden übermittelt werden, wenn der Auskunftsbeghernde ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft macht. Die Übermittlung weiterer Daten ist nur aufgrund eines rechtlichen Interesses zulässig. Da aus dem Internet jeder Daten abrufen kann, ohne daß er hierfür seine Gründe darlegen muß, hat die Gemeinde keine Möglichkeit, festzustellen, ob die Voraussetzungen für eine

Datenübermittlung nach § 14 Abs. 8 GewO gegeben sind. Eine Übernahme von Gewerberegisterdaten ins Internet ohne Einwilligung des Betroffenen hat daher zu unterbleiben.

14. Statistik

14.1 EU-Vorhaben einer Volks-, Gebäude- und Wohnungszählung 2001

Auf EU-Ebene wird seit geraumer Zeit das Vorhaben eines gemeinschaftsweiten Zensus im Jahr 2001 diskutiert. Inzwischen wurde von Seiten der EU ein Leitlinienentwurf vorgelegt. Dieser Entwurf empfiehlt den Mitgliedsstaaten der EU im Jahre 2001 eine Volks-, Gebäude- und Wohnungszählung durchzuführen und dabei in der Leitlinie näher definierte sogenannte Kernvariablen zu erfassen. Auch wenn durch die rechtlich relativ wenig verbindlichen Leitlinien ein Teilnahmezwang nicht begründet wird, bestehen nach meiner Kenntnis von Seiten der Bundesrepublik Deutschland keinerlei Erwägungen für eine Nichtteilnahme. Die Bundesregierung hat sich allerdings aus Kosten- und Akzeptanzgründen gegen eine traditionelle Volkszählung ausgesprochen. Es wird vielmehr daran gedacht, vorhandene administrative und statistische Daten zu nutzen. Es werden augenblicklich zwei Modellvarianten diskutiert.

Im Modell I werden demographische Grunddaten (Alter, Geschlecht usw.) aus dem Melderegister gewonnen, erwerbsstatistische Daten aus bestehenden Beschäftigungsstatistiken und ergänzende Angaben aus dem Mikrozensus. Bei dieser Modellvariante erfolgt keine personen- oder einzelfallbezogene Verknüpfung und demgemäß auch keine entsprechende Auswertung.

Das Modell II sieht eine Kombination aus der Nutzung vorhandener Register (z.B. wie im Modell I dem Melderegister) und Primärerhebungen in den Bereichen vor, die durch Registerdaten nicht abgedeckt sind. So soll bspw. eine postalische Befragung der Gebäudeeigentümer für Zwecke einer Gebäude- und Wohnungszählung erfolgen. Entscheidend ist, dass bei diesem Modell die erfaßten Daten zu Personendatensätzen zusammengeführt werden sollen und auch eine Auswertung in feiner regionaler Gliederung erfolgen soll.

Aus datenschutzrechtlicher Sicht ist im augenblicklichen Stand der Überlegungen folgendes anzumerken:

- Unabhängig vom letztendlich gewählten Verfahren bedarf eine derartige Erhebung einer den Anforderungen des Volkszählungsurteils entsprechenden bundesgesetzlichen Grundlage.
- Eine Ergänzung der in Frage stehenden Verwaltungsregister um weitere Merkmale, welche letztendlich nicht für die rechtmäßige Erfüllung von Verwaltungsaufgaben erforderlich sind, sondern nur für statistische Zwecke Verwendung finden sollen, wäre unzulässig.
- Eine Verknüpfung der vorhandenen Verwaltungs- und Statistikdaten zu Einzeldatensätzen läßt die Verwendung eines personenkennzeichenähnlichen Schlüssels denkbar erscheinen. Der Einsatz eines derartigen Kennzeichens ist vom Bundesverfassungsgericht im Volkszählungsurteil als nicht zulässig angesehen worden. Nach Ansicht des Gerichts wäre dies ein entscheidender Schritt, den einzelnen Bürger in seiner gesamten Persönlichkeit zu registrieren und zu katalogisieren.
- Bei beiden Modellvarianten wird in nicht unerheblichem Umfang zur Klärung von Zweifelsfällen eine Nachprüfung vor Ort durch Beschäftigte der Statistischen Landesämter erfolgen müssen. Es muß zuverlässig ausgeschlossen sein, daß die Ergebnisse der Nachprüfung, welche im statistischen Bereich anfallen, in die Verwaltung zurückfließen. Die Abschottung des Statistikbereichs von Verwaltungsvollzug stellt eine zentrale Maßgabe im Urteil des Bundesverfassungsgerichts dar.

14.2 Nutzung von Statistikdaten für den Verwaltungsvollzug

Im Rahmen einer Eingabe wurde ich darauf aufmerksam gemacht, daß eine Gemeinde die von einem Gemeindebürger in Erfüllung seiner agrarstatistischen Auskunftspflicht gemachten Angaben für Zwecke einer vorzeitigen Besitzeinweisung nach Art. 39 Bayerisches Enteignungsgesetz verwendet hatte. Nach Überprüfung stellt sich die Sachlage wie folgt dar:

Für die im Rahmen des agrarstatistischen Erhebungsprogramms befragten land- und forstwirtschaftlichen Betriebe ordnet das Agrarstatistikgesetz eine Auskunftspflicht an. Zur Durchführung der Erhebung können vor Ort Erhebungsstellen eingerichtet werden, wobei die nähere Ausgestaltung dieser Erhebungsstellen den Landesregierungen durch Rechtsverordnung obliegt. Die Bayerische Staatsregierung hat durch die Agrarstatistikverordnung die Einrichtung von örtlichen Erhebungsstellen bei den Gemeinden angeordnet und für diese Erhebungsstellen die Vorschriften des Bayerischen Statistikgesetzes für anwendbar erklärt. Danach sind diese Erhebungsstellen räumlich und organisatorisch in der Zeitspanne vom Eingang der Erhebungsunterlagen bis zu deren Ablieferung an das Landesamt für Statistik und Datenverarbeitung von anderen Verwaltungsstellen zu trennen. Die in den Erhebungsstellen tätigen Personen dürfen statistische Einzelangaben und gelegentlich ihrer Tätigkeit gewonnene Erkenntnisse nicht in anderen Verfahren verarbeiten oder nutzen, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist. Eine solche Rechtsvorschrift besteht in dem zu beurteilenden Sachverhalt nicht.

15. Schulwesen

15.1 Lehrerdaten und Daten der Elternbeiratsmitglieder im Internet

Eine Lehrkraft hat mir vorgetragen, daß ohne ihre vorherige Information und Zustimmung ihr Name und ihre Sprechstunden sowie die Namen und Adressen des Elternbeirats in der Homepage der Schule veröffentlicht worden waren.

Ich habe der Schule mitgeteilt, daß im Hinblick auf die enge lokale Begrenzung des Aufgaben- und Wirkungsbereichs von Schulen das Persönlichkeitsrecht der Lehrer und Eltern Vorrang vor dem Informationsinteresse der Internetnutzer habe.

Daher ist vor Einstellung der genannten Daten ins Internet die Einwilligung der Betroffenen einzuholen; dies gilt natürlich auch für Schulsehörer, die keine unmittelbar nach außen wirkende Tätigkeit wahrnehmen (z.B. Hausmeister, Sekretärin).

Auf den Beitrag zum Thema "Mitarbeiterdaten im Internet" in [Nr. 12.3](#) dieses Tätigkeitsberichts darf ich verweisen

15.2 Datenerhebung bei Erkrankung von Schülern

In einer Eingabe haben mir Eltern vorgetragen, daß in der Schule ihres Kindes ein Rundschreiben verteilt wurde, in dem Vorgaben gemacht wurden, wie sich die Schüler bei einer Erkrankung zu verhalten hätten. Unter anderem mußte bei allen Erkrankungen die **Art** der Erkrankung angegeben werden; eine Ausnahme bildete lediglich das ärztliche Attest.

Ich vertrete hierzu die Auffassung, daß für die Forderung nach Angabe der Art der Erkrankung keine Rechtsgrundlage besteht. Auch in ärztlichen Attesten braucht die Art der Erkrankung nicht angegeben zu werden. Unabhängig davon kann in Einzelfällen eine freiwillige Mitteilung über die Art der Erkrankung an die Schule nützlich sein und die Fürsorge der Schule für den Schüler erleichtern.

Unberührt davon bleiben die Bestimmungen des Bundesseuchengesetzes und die entsprechenden Meldepflichten.

Ich habe die Schule aufgefordert, auf die Erhebung zu verzichten bzw. auf die Freiwilligkeit der Angabe hinzuweisen.

15.3 Weitergabe gesundheitlicher Daten aus Schuluntersuchungen im Rahmen der Schulgesundheitspflege an die Schulleitung

Das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit hat mir die Frage gestellt, inwieweit die Gesundheitsämter der jeweiligen Schulleitung die Ergebnisse von Schuluntersuchungen, insbesondere der **Einschulungsuntersuchungen**, mitteilen dürfen. Ich habe auf folgendes hingewiesen:

- Auch bei einer Schuluntersuchung gilt die **ärztliche Schweigepflicht** gemäß § 203 Abs. 1 StGB. Die Gesundheitsämter geben den Schulleitungen jedoch gemäß Art. 80 Abs. 3 Satz 2 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) die notwendigen Hinweise, soweit aus dem Untersuchungsergebnis **Folgerungen für die Unterrichtsgestaltung** zu ziehen sind.
- Gemäß Art. 80 Abs. 3 Satz 2 BayEUG ist es daher zulässig, wenn der Schulleitung das **Gesamtergebnis** der Untersuchung, z.B. ob das Kind schulfähig ist oder nicht, mitgeteilt wird.

- Für die Unterrichtsgestaltung bedeutsame Ergebnisse, die der Schulleitung mitgeteilt werden können, sind beispielsweise eine Schwerhörigkeit oder eine Sehschwäche. Sofern nicht besondere Umstände vorliegen, sollten aber die Erziehungsberechtigten darüber unterrichtet werden, welche Mitteilungen an die Schulleitung erfolgen und warum diese Mitteilungen im konkreten Fall für erforderlich gehalten werden. Aus datenschutzrechtlicher Sicht ist es wünschenswert, die Kenntnisnahme durch die Erziehungsberechtigten anzustreben.
- Bei Schülern, die aufgrund einer Erkrankung (z.B. Diabetes, Epilepsie) einer **besonderen gesundheitlichen Gefährdung** ausgesetzt sind und in einem Notfall besonderer Hilfsmaßnahmen bedürfen, kann im Einzelfall auch die Angabe der Diagnose im engeren Sinn erforderlich sein. Hier dürfte jedoch funktionellen Angaben, z.B. Leistungs- und Funktionseinschränkungen (Verlängerung der Pausen, Aussetzen bei bestimmten Unterrichtseinheiten z.B. Sport etc.), der Vorzug zu geben sein. Für medizinische Laien ist es wichtiger, zu wissen, durch welche Anzeichen sich die Krankheit äußert und worauf bei den zu treffenden Sofortmaßnahmen zu achten ist, als eine Diagnose zu kennen.
- Die Tatsache einer **HIV-Infektion** muß aus medizinisch-fachlicher Sicht der Schule nicht bekannt sein, da hiervon bei Kontakten, wie sie in Schulen beim Unterricht üblich sind, keine besondere Ansteckungsgefahr ausgeht. Anders liegen dagegen die Verhältnisse bei einer **ausgebrochenen Aids-Erkrankung**. Da dies aus medizinisch-fachlicher Sicht notwendig ist, dürfen in diesem Fall die funktionellen Einschränkungen mitgeteilt werden, auf die Rücksicht zu nehmen ist. Die Mitteilung der Diagnose ist jedoch in der Regel nicht erforderlich. Sollte diese ausnahmsweise dennoch für erforderlich gehalten werden, empfehle ich, die Einwilligung der Erziehungsberechtigten einzuholen. Sollte es Fälle geben, in denen eine Mitteilung der Diagnose erforderlich ist, obwohl sich die Erziehungsberechtigten dagegen aussprechen, sind diese über die Mitteilung zu informieren.

16. Verkehrswesen

16.1 Parkausweise für Schwerbehinderte

Wie bereits in früheren Jahren wurde ich im Berichtszeitraum erneut mit der Frage befaßt, ob es zulässig ist, auf der Vorderseite der Ausweise für Parkerleichterungen für Schwerbehinderte, die beim Parken auf Schwerbehinderten-Parkplätzen sichtbar auszulegen sind, den jeweiligen Namen einzutragen. Aus diesem Anlaß weise ich auf folgendes hin:

Das Aussehen und der Inhalt des Parkausweises für Schwerbehinderte ist in der Vollzugsbekanntmachung zur Straßenverkehrs-Ordnung (VollzBek-StVO) vom 9. August 1991, AllMBI S. 650, geregelt. Zu den einzutragenden Daten gehört auch der Name des Inhabers. Falls ein Behinderter mit der Nennung seines Namens auf der Vorderseite des Ausweises dennoch nicht einverstanden ist, sieht die VollzBek-StVO vor, auf seinen Wunsch das Namensfeld freizulassen und den Namen auf der Rückseite des Ausweises einzutragen. In diesem Fall soll der Berechtigte jedoch darauf aufmerksam gemacht werden, daß der Ausweis im Ausland möglicherweise nicht anerkannt wird. Um diesem Problem abzuhelpfen, ist es auch zulässig, auf Antrag einen Ausweis mit Namenseintragung sowohl auf der Vorder- als auch auf der Rückseite auszustellen. Im Inland kann der Berechtigte das Namensfeld auf der Vorderseite abdecken, bei Auslandsaufenthalten kann die Abdeckung entfernt werden.

16.2 Auskunftserteilung der Kfz-Zulassungsstellen gegenüber dem Bayerischen Rundfunk

Die Abteilung Rundfunkgebühren des Bayerischen Rundfunks hat gegenüber der Kfz-Zulassungsstelle eines Landratsamtes die Auffassung vertreten, der Betrieb eines Autoradios stünde im Zusammenhang mit der Teilnahme am Straßenverkehr, weil das Autoradio u.a. für Verkehrsdurchsagen und Staumeldungen genutzt wird und dadurch den Autofahrern und den für den Straßenverkehr zuständigen Behörden erhebliche Vorteile bietet. Das Landratsamt sei daher nach § 39 Abs. 1 des Straßenverkehrsgesetzes (StVG) berechtigt, einem Beauftragten für Rundfunkgebühren des Bayerischen Rundfunks die von diesem erbetenen Halterauskünfte zu erteilen. Außerdem äußerte die Abteilung Rundfunkgebühren des Bayerischen Rundfunks die Ansicht, daß eine Halterauskunft auch nach § 39 Abs. 3 StVG zulässig wäre, da die Halterdaten zur Geltendmachung des öffentlich-rechtlichen Anspruchs auf Anmeldung der gebührenpflichtigen

Rundfunkgeräte und Zahlung der entsprechenden Rundfunkgebühren benötigt würden.

Ich halte diese Rechtsauffassung in Übereinstimmung mit dem Bayerischen Staatsministerium für Wirtschaft, Verkehr und Technologie für unzutreffend:

Gem. Nr. 4 a.E. des Merkblattes für Anfragen und Auskünfte aus den Fahrzeugregistern nach § 39 Abs. 1 und 2 StVG (VkBl. 1993, 525, 527) ist der Zusammenhang mit der Teilnahme am Straßenverkehr insbesondere bei Auskunftersuchen von Rundfunkanstalten zur Ausfindigmachung von Schuldnern von Rundfunkgebühren (Autoradio) zu verneinen. Im übrigen sind die Rundfunkgebührenansprüche des Bayerischen Rundfunks bereits deshalb keine Rechtsansprüche im Zusammenhang mit der Teilnahme am Straßenverkehr, da die Rundfunkgebührenpflicht allein vom Bereithalten eines Rundfunkempfangsgeräts abhängt und diese auch dann entstehen würde, wenn das Kraftfahrzeug, in das das Autoradio eingebaut ist, nicht zugelassen wäre (vgl. § 2 Abs. 2, § 1 Abs. 3 Satz 2 des Rundfunkgebührenstaatsvertrages). Eine Halterauskunft nach § 39 Abs. 1 StVG an den Bayerischen Rundfunk bzw. an einen seiner Beauftragten für Rundfunkgebühren ist daher unzulässig.

Dies gilt auch für eine Datenübermittlung nach § 39 Abs. 3 StVG. Der Bayerische Rundfunk müßte dazu gegenüber der Zulassungsstelle glaubhaft machen, daß die Daten zur Geltendmachung von Ansprüchen in Höhe von mindestens 1000 DM benötigt werden. Dies wird jedoch regelmäßig nicht möglich sein, da die Frage, ob und ggf. in welcher Höhe ein Anspruch vorliegt, erst dann beantwortet werden kann, wenn feststeht, daß die Voraussetzungen für das Entstehen einer Rundfunkgebührenbeitragspflicht bei dem betreffenden Fahrzeughalter vorliegen. Eine Prüfung dahingehend kann jedoch erst dann erfolgen, wenn der Halter des Fahrzeugs bekannt ist. Gerade diese Daten sollen jedoch durch die Anfrage bei der Kraftfahrzeugzulassungsstelle erst ermittelt werden.

Hat der Bayerische Rundfunk zureichende tatsächliche Anhaltspunkte für das Vorliegen einer Ordnungswidrigkeit kann er bei der zuständigen Kreisverwaltungsbehörde die Durchführung eines Ordnungswidrigkeitenverfahrens anregen. In diesem Fall kann er der Kreisverwaltungsbehörde das Kfz-Kennzeichen mitteilen und diese erhält von der Zulassungsstelle gemäß § 35 Abs. 1 Nr. 3 StVG die notwendige Halterauskunft.

17. Medien

17.1 Benutzung dienstlicher Telekommunikationsanlagen

Mit dem Inkrafttreten des Telekommunikationsgesetzes am 25.7.1996 (vgl. [17. TB, Nr. 17.1](#)) waren auch die Auswirkungen auf bestehende innerdienstliche Vorschriften über die Inanspruchnahme von dienstlichen Telefonanlagen durch Beschäftigte zu überprüfen.

Die Prüfung ergab folgende Rechtslage:

Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war ([§ 85 Abs. 1 TKG](#)).

Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt ([§ 85 Abs. 2 TKG](#)).

Den Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen ([§ 85 Abs. 3 TKG](#)).

Die vorgenannten Bestimmungen stehen unter keinem weiteren Vorbehalt. Damit besteht wegen der ausschließlichen Gesetzgebungskompetenz des Bundes für die Telekommunikation (§ 73 Nr.7 GG) keine Möglichkeit für eine (abweichende) landesspezifische Regelung.

Auch für anderslautende Regelungen in Dienst- oder Betriebsvereinbarungen ist kein Raum. Solche Vereinbarungen sind nur zulässig, soweit eine gesetzliche (oder tarifliche) Regelung nicht besteht (vgl. Art. 73 BayPVG).

Ausdrücklich unterliegen nach der amtlichen Begründung zum TKG "..... **Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind**" dem Fernmeldegeheimnis.

Nach [§ 89 Abs. 2 Nr. 1 c\) TKG](#) dürfen Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, die Daten natürlicher Personen erheben, verarbeiten und nutzen, soweit dies erforderlich ist für das ordnungsgemäße Ermitteln und den Nachweis der Entgelte.

Bezogen auf die vom Arbeitgeber geduldete **private** Nutzung von dienstlichen Telekommunikationseinrichtungen ergibt sich damit ein sehr enger Handlungsrahmen für die Abrechnung. Die Kenntnisnahme einzelner Verbindungsdaten privater Telekommunikationsvorgänge ist für den Arbeitgeber im Regelfall nicht erforderlich; er hat ein Verfahren zu entwickeln, das diesen Vor-

gaben gerecht wird.

Die Rechtslage bei Nebenstellenanlagen, soweit sie von Beschäftigten aus **dienstlichem** Anlaß in Anspruch genommen werden, unterscheidet sich deutlich vom Obengesagten.

In solchen Fällen tritt der Arbeitgeber nicht als Anbieter von Telekommunikation für Dritte auf, er ist vielmehr aus der Sicht der gewerblichen Telekommunikationsunternehmen Endnutzer (Kunde). Die Beschäftigten sind gegenüber ihrem Arbeitgeber nicht Dritte, sie handeln vielmehr weisungsgebunden für ihn auch im Telekommunikationsverkehr. Der Arbeitgeber wirkt unmittelbar auf das dienstliche Telekommunikationsverhalten der Beschäftigten ein, er kann die Aufnahme einer entsprechenden Verbindung im Rahmen seiner Direktionsbefugnis anordnen, verbieten oder auch überwachen (vgl. Feuerwehrnotruf, Rettungsdienst). Telekommunikation ist hier nicht Geschäftszweck, sondern Hilfsmittel zur Durchführung der originären Aufgaben. Fehlt es indes an der geschäftsmäßigen Erbringung von Telekommunikationsdiensten, so ist der 11. Teil des TKG nicht unmittelbar anwendbar ([§ 85 Abs. 2 TKG](#)).

Dem Arbeitgeber öffnet sich damit ein Handlungsrahmen, in dem er von seinem Direktionsrecht und seinen Überwachungsbefugnissen gegenüber seinen Beschäftigten Gebrauch machen kann. Dazu gehört auch die Möglichkeit der Auswertung von Verbindungsdaten bei dienstlich veranlaßten Telekommunikationsvorgängen, unter Umständen sogar auch die inhaltliche Auswertung der Telekommunikation selbst.

Die Grenzen der Zulässigkeit solchen Handelns ergeben sich aus einer Abwägung der berechtigten Interessen des Arbeitgebers mit den schutzwürdigen Belangen des Beschäftigten. Dabei sind auch die Grundsätze des 11. Teils des TKG (insbesondere [§§ 85, 87, 89 TKG](#)) vergleichend heranzuziehen. Einer allgemeingültigen Regelung steht die Vielgestaltigkeit der Arbeitsplätze und die Funktionsvielfalt der Arbeitnehmertätigkeit entgegen. Auch sind Besonderheiten bei bestimmten Funktionen zu beachten (Drogenberater, Personalratstätigkeit u.a.).

Die berechtigten Belange der Beschäftigten sind zu berücksichtigen. Die Rechtsprechung zum Arbeitnehmerdatenschutz ist daher zu beachten. **Ferner ist die Mitbestimmung der jeweiligen Arbeitnehmervertretung (Betriebs- bzw. Personalrat) zwingende Voraussetzung für die Zulässigkeit der genannten Maßnahmen.** Ohne ordnungsgemäße Beteiligung der Arbeitnehmervertretung, die zu einer Dienst- oder Betriebsvereinbarung führen kann - aber nicht muß - ist eine Datenerhebung über Telekommunikationsvorgänge unzulässig.

Bei Regelungen der vorgenannten Art sind auch die Persönlichkeitsrechte der außenstehenden

Telekommunikationsteilnehmer (B-Teilnehmer) zu beachten. Es ist jedoch zu berücksichtigen, daß das Fernmeldegeheimnis nicht für die (End-)Nutzer von Telekommunikationsverbindungen gilt. Wie bereits erwähnt, tritt im Regelfall bei dienstlich veranlaßten Verbindungen der Arbeitgeber als Teilnehmer auf; seine Beschäftigten sind insoweit Erfüllungsgehilfen. Damit steht dem Arbeitgeber auch grundsätzlich das Recht zu, sich über den B-Teilnehmer zu informieren und Aufzeichnungen über die näheren Umstände der Telekommunikation zu machen.

Dies gilt nicht, wenn besondere berufliche Verschwiegenheitspflichten dem Beschäftigten verbieten, seinem Arbeitgeber Kenntnis über Personen zu verschaffen, mit denen er im Rahmen seiner Tätigkeit Kontakt hat (z.B. freiwillige Drogenberatung). Der Arbeitgeber tritt hier nicht als Teilnehmer auf. Auch bei privaten Telekommunikationsverbindungen fehlt es an der Teilnehmereigenschaft des Arbeitgebers. In beiden Fällen ist daher die Verarbeitung von Daten über den B-Teilnehmer durch den Arbeitgeber unzulässig. In den übrigen Fällen ist der Erforderlichkeitsgrundsatz zu beachten.

Für die bayerische Staatsverwaltung wurden am 7. November 1997 neu gefaßte Dienstanschlußvorschriften (BayDAV) veröffentlicht (FMBI. Nr. 14 Seite 280 ff), die der oben beschriebenen Rechtslage entsprechen. Meine Anregungen dazu wurden berücksichtigt.

18. Umweltfragen

18.1 Videoüberwachung kommunaler Wertstoffhöfe und Containerstandorte

Um unerlaubten Abfallablagerungen auf Wertstoffhöfen und Containerstandorten zu begegnen, wird von entsorgungspflichtigen Körperschaften der Einsatz einer Videoüberwachung derartiger Standorte in Betracht gezogen. Ich halte es aus den folgenden Überlegungen für erforderlich, durch Hinweisschilder auf die Videoüberwachung aufmerksam zu machen:

1. Der Einsatz der Videotechnik zur Beobachtung und Erfassung aufgezeichneter Personen stellt einen Eingriff in das durch Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG gewährleistete Recht auf informationelle Selbstbestimmung dar, der einer ausreichenden Rechtsgrundlage bedarf.
2. Eine spezialgesetzliche Befugnis für die Videoüberwachung kommunaler Wertstoffhöfe und Containerstandorte besteht nicht. Die Zulässigkeit der Videoüberwachung richtet

sich somit nach dem Bayerischen Datenschutzgesetz ([Art. 15 Abs. 1 Nr. 1 BayDSG](#)).

- a. Die Erhebung personenbezogener Daten mittels Videoaufnahmen ist nach [Art. 16 Abs. 1 BayDSG](#) zulässig, wenn die Aufnahme zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Erforderlich ist die Erhebung von Daten dann, wenn ihre Kenntnis zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch als angemessen erscheint (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rdnr. 9).

Mit der Videoüberwachung von Wertstoffhöfen wird der Zweck verfolgt, eine ordnungsgemäße Benutzung der Wertstoffhöfe sicherzustellen, illegale Ablagerungen zu verhindern und Verstöße gegen das Abfallrecht aufzuklären. Personen, die an diesen Orten illegale Ablagerungen vornehmen, können festgestellt werden, wenn sie mit einem Kraftfahrzeug vorfahren, und die Videokamera neben dem Vorgang der illegalen Ablagerung das Kfz-Kennzeichen aufzeichnet. Das Verfahren ist also geeignet. Dazu trägt es bei offener Überwachung dazu bei, der Begehung von Ordnungswidrigkeiten durch unerlaubte Ablagerungen vorzubeugen und illegale Ablagerungen zu vermeiden.

Bei der Frage der Angemessenheit von Videoaufnahmen im Verhältnis zu dem angestrebten Zweck sind folgende Gesichtspunkte zu berücksichtigen:

- Die Videoüberwachung von Wertstoffhöfen stellt wie bemerkt einen Eingriff in das Recht auf informationelle Selbstbestimmung der überwachten Personen dar. Die Videokamera wird dabei nicht nur zur -räumlich versetzten- Überwachung über einen oder mehrere Bildschirme von zentraler Stelle aus eingesetzt. Es werden vielmehr permanent Videoaufzeichnungen gefertigt, die im nachhinein betrachtet und ausgewertet werden können. Ein solcher Eingriff hat eine andere Qualität als eine Beobachtung ohne Aufzeichnung.

- Von der Videoüberwachung sind alle Personen betroffen, die in den Erfassungsbereich der Kamera gelangen. Es werden also nicht nur die Personen aufgezeichnet, die illegal Ablagerungen vornehmen, sondern auch alle anderen, die sich dort rechtmäßig aufhalten. Diese haben ein berechtigtes Interesse daran, nicht heimlich registriert zu werden. Demgegenüber können sich Personen, die Ordnungswidrigkeiten begehen, nicht auf schutzwürdige Belange berufen, wenn sie zur Ermittlung der Ordnungswidrigkeit aufgezeichnet werden.
- Durch eine Videoüberwachung kann die Begehung von Ordnungswidrigkeiten durch illegale Ablagerungen verhindert werden, wenn auf die Überwachung durch Hinweisschilder aufmerksam gemacht wird. Es wäre deshalb unangemessen, wenn die Kommune die Begehung von Ordnungswidrigkeiten zulassen würde, um die Umweltsünder anschließend durch die Videoaufnahme zu überführen, obwohl durch einen Hinweis auf die Videoüberwachung die Ordnungswidrigkeiten hätten vermieden werden können. Die Kommune ist daher zu einem Hinweis verpflichtet, wenn sie auf ihrem Wertstoffhof die Videotechnik einsetzt.
- Im Ergebnis ist der Einsatz der Videotechnik auf Wertstoffhöfen und Containerstandorten somit grundsätzlich geeignet, illegale Ablagerungen an diesen Orten aufzuklären. Die Personen, die sich rechtmäßig verhalten, haben jedoch ein schutzwürdiges Interesse daran, daß sie nicht heimlich aufgezeichnet werden. Ein Hinweis auf die Videoüberwachung ist außerdem geboten, um die Begehung von Ordnungswidrigkeiten zu verhindern. Die Videoüberwachung von Wertstoffhöfen ist daher nur dann auch angemessen und damit nach [Art. 16 Abs. 1 Satz 1 BayDSG](#) erforderlich, wenn durch Hinweisschilder auf die Videoüberwachung aufmerksam gemacht wird.

- b. Zu berücksichtigen ist vor allem, daß nach dem Bayerischen Datenschutzgesetz personenbezogene Daten primär beim Betroffenen mit seiner Kenntnis zu erheben sind ([Art. 16 Abs. 2 Satz 1 BayDSG](#)). Eine Datenerhebung beim Betroffenen ohne seine Kenntnis ist nur zulässig, wenn eine Rechtsvorschrift eine solche Erhebung vorsieht oder zwingend voraussetzt oder die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder im Einzelfall eine solche Erhebung erforderlich macht ([Art. 16 Abs. 2 Satz 3 BayDSG](#) i.V.m. [Art. 16 Abs. 2 Satz 2 Nrn. 1 und 2 a BayDSG](#)).

Eine Rechtsvorschrift, die Videoaufnahmen auf Wertstoffhöfen ohne Kenntnis der Betroffenen vorsieht oder voraussetzt, besteht nicht. Zur Vermeidung illegaler Ablagerungen ist es auch nicht erforderlich, eine Videoüberwachung von Wertstoffhöfen ohne Kenntnis der betroffenen Bürger durchzuführen. Das Aufstellen von Hinweisschildern, mit denen auf die Videoüberwachung aufmerksam gemacht wird, ist im Gegenteil dazu geeignet, potentielle Umweltsünder von illegalen Ablagerungen abzuhalten und damit Ordnungswidrigkeitentatbestände erst gar nicht entstehen zu lassen. Heimliche Aufnahmen sind deshalb aus datenschutzrechtlichen Gründen unzulässig.

Neben den Hinweisschildern sind folgende Grundsätze zu beachten:

- Die Überwachung ist auf den von illegalen Müllablagerungen betroffenen Bereich (das kann auch der gesamte Wertstoffhof sein) zu begrenzen.
- Sofern keine unerlaubten Müllablagerungen festzustellen sind, dürfen Aufzeichnungen nicht ausgewertet werden; sie sind unverzüglich zu löschen. Auch im übrigen sind die Aufzeichnungen zu löschen, sobald sie zur Feststellung von Betroffenen und zur Beweissicherung nicht mehr erforderlich sind.

18.2 Weitergabe von Prüftagebüchern durch Sachverständigen-Organisationen an das Bayerische Landesamt für Wasserwirtschaft

Kurz hintereinander haben sich zwei amtlich anerkannte Sachverständigen-Organisationen gem. § 22 der Verordnung über Anlagen zum Umgang mit wassergefährdenden Stoffen und über Fachbetriebe (Anlagenverordnung-VAwS) an mich mit der Frage gewandt, ob sie verpflichtet seien, dem Bayerischen Landesamt für Wasserwirtschaft die von ihnen geführten Prüftagebücher auf dessen Verlangen vorzulegen. Ich habe ihnen daraufhin folgendes geantwortet:

Die Pflicht der Sachverständigen-Organisationen, die Prüftagebücher aller ihrer in Bayern tätigen Sachverständigen jeweils zum 01.03. eines Jahres dem Landesamt für Wasserwirtschaft vorzulegen, ist in § 22 Abs. 5 Satz 3 Halbsatz 2 VAwS geregelt. In diesen Aufzeichnungen, die auch personenbezogene Daten enthalten (z.B. über den Betreiber der überprüften Anlage), haben die Sachverständigen alle wesentlichen bei ihren Prüfungen gewonnenen Erkenntnisse zu vermerken. Die Vorlage der Prüftagebücher ist erforderlich, damit sich das Landesamt für Wasserwirtschaft im Rahmen seiner Aufsichtspflicht über die Sachverständigen-Organisationen (vgl. § 22 Abs. 1 Satz 5 VAwS) einen Überblick über deren Tätigkeit verschaffen und ggf. die notwendigen Maßnahmen gegenüber den Organisationen treffen kann. Gegen die Übersendung der Prüftagebücher an das Landesamt für Wasserwirtschaft bestehen daher keine datenschutzrechtlichen Bedenken.

18.3 Datenübermittlung aus der Anlagenkartei an Sachverständigen-Organisationen für Wasserwirtschaft

Eine amtlich anerkannte Sachverständigen-Organisation gem. § 22 der Verordnung über Anlagen zum Umgang mit wassergefährdenden Stoffen und über Fachbetriebe (Anlagenverordnung-VAwS) hat mich um Auskunft gebeten, ob ihr die von den Kreisverwaltungsbehörden geführte Anlagenkartei nach § 24 VAwS zugänglich sei. Dies wurde von mir verneint.

Die Zulässigkeit der Datenübermittlung aus der Anlagenkartei richtet sich mangels spezialgesetzlicher Regelungen nach [Art. 19 Abs. 1 Nr. 2 BayDSG](#). Sie setzt danach voraus, daß der Auskunftersuchende ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegen kann und der Betroffene kein schutzwürdiges Interesse am Ausschluß der Übermittlung hat.

Ein berechtigtes Interesse der Sachverständigen-Organisation an der Übermittlung der Anlagenkartei vermochte ich jedoch nicht zu erkennen. Zum einen ist der Prüfauftrag vom Betreiber einer wassergefährdenden Anlage an eine anerkannte Sachverständigen-Organisation zu erteilen (Nr. 23.1.1 der Verwaltungsvorschrift zum Vollzug der Anlagenverordnung-VVAwS-). Zum anderen kann diese die für die Prüfung notwendigen Angaben beim Betreiber selbst erfragen. Es ist daher nicht erforderlich, daß eine Sachverständigen-Organisation die Daten über die von ihr zu prüfenden Anlagen und ihre Betreiber aus der Anlagenkartei erhält. Sollte die Datenübermittlung Werbezwecken dienen, läge zwar ein berechtigtes Interesse vor, sie wäre aber dennoch unzulässig, da sie die schutzwürdigen Belange der Betroffenen, von personenbezogenen Werbemaßnahmen verschont zu bleiben, beeinträchtigen würde.

19. Technischer und organisatorischer Bereich

19.1 Technische Grundsatzfragen

19.1.1 Entwicklung der automatisierten Datenverarbeitung

Nach dem ersten Bayer. Datenschutzgesetz vom 28.4.1978 traten zum 1.1.1979 die Bestimmungen über die technischen und organisatorischen Datensicherungsmaßnahmen in Kraft. Ein knappes Jahr hatte man den datenverarbeitenden Stellen Zeit gegeben, geeignete Sicherungsmaßnahmen einzuführen.

In den vergangenen 20 Jahren hat sich das Erscheinungsbild der automatisierten Datenverarbeitung dramatisch verändert. Während in den "Anfängen des Datenschutzes" in erster Linie die Großrechner die automatisierte Datenverarbeitung prägten, haben wir es heute mit einer Vielzahl von Rechnern unterschiedlicher Größe und Funktion zu tun. Die nahezu unbegrenzten Vernetzungsmöglichkeiten bedeuten für die Datenschutzbeauftragten und die Revisionsinstanzen bei ihren Kontrollaufgaben eine große Herausforderung. Durch die modernen Programmierwerkzeuge ist eine Programmkontrolle in der herkömmlichen Art, als man noch Einsicht in den Sourcecode nahm, heute nicht mehr sinnvoll und erfolgversprechend. In der Client/Server-Umgebung wird mit Standardprodukten und Anwendungssystemen von unterschiedlichen Herstellern oder Softwarehäusern gearbeitet, daß selbst die Anwender bei der Fehlerbehebung oder bei kleinsten Änderungen auf die Hilfe Fremder angewiesen sind. Ob dann bei solchen Eingriffen Verstöße gegen die Datensicherheit oder den Datenschutz - durch die Kenntnisnahme geschützter perso-

nenbezogener Daten - aufgetreten sind, läßt sich - bei fehlender Protokollierungsmöglichkeit - meist nicht feststellen.

Die Datenverarbeitung wird also zunehmend unübersichtlicher. Vielerorts unternimmt man zwar Anstrengungen, wieder mehr Transparenz in die Datenverarbeitung zu bringen, manche Anwender haben jedoch schon den Überblick verloren oder wollen nicht mehr so viele Ressourcen in die automatisierte Datenverarbeitung stecken und nehmen die oft günstigen Angebote von externen Dienstleistern in Anspruch (Outsourcing).

Anfang 1997 fand in den Vereinigten Staaten eine repräsentative Umfrage zum Thema "Sicherheit und Verfügbarkeit der automatisierten Datenverarbeitung" statt, an der sich etwa 2000 Unternehmen beteiligten (MERIT-Studie, Maximizing the Efficiency of Resources in Information Technology). Das Ergebnis überrascht eigentlich nicht: Mainframe-Architekturen wurden weit zuverlässiger eingeschätzt als Systeme in verteilten Client/Server-Umgebungen. 70 Prozent der Unternehmen, die Großrechner einsetzen, haben Verfügbarkeitswerte von über 99,5 Prozent, hingegen können nur 55 Prozent, die mit Client/Server-Umgebungen arbeiten, mit gleicher Verfügbarkeit aufwarten. Als Gründe für das bessere Abschneiden des Großrechners wurden geringere Ausfallzeiten, als Folge stabilerer Software, und bessere Wiederherstellungsmechanismen genannt. Die Ausfälle der Client/Server-Systeme hatten ihren Grund meist in Anwendungsfehlern, in Fehlern in der Software, in einer unzureichenden Änderungskontrolle oder in der fehlenden Prozeßautomation. Überlastung, vorher nicht erkannte Spitzenlasten und ungenügende Bandbreiten wurden als Gründe für die Netzwerkausfälle genannt. Die Ausfälle bei den Datenbanken resultierten häufig aus unzureichenden Speicherkapazitäten, vollen Protokolldateien oder sonstigen Überlastungen. Die Anwendungsfehler waren auf eine ebenfalls unzureichende Änderungskontrolle, auf Betriebsfehler oder mangelnde Automatisierung zurückzuführen. Führende Softwarehäuser haben deshalb auf diese Erscheinung reagiert und bieten plattformübergreifende Softwareprodukte zur Steuerung und Überwachung dieser Systemumgebungen an. Alle Probleme lassen sich jedoch auch mit diesen Produkten nicht lösen.

Viele, vor allem kleinere Anwender werden jedoch weiterhin mit diesen Problemen leben müssen, weil sie sich keinen Großrechner leisten können und über keine Fachleute verfügen, die eine so komplexe Steuerungs- und Überwachungssoftware bedienen können. Denn der Betreuungsaufwand einer solchen Software ist nicht zu unterschätzen und die Personaldecke in der Informationstechnik ist häufig dünn. Auf den Einsatz der Datenverarbeitung zu verzichten, kann sich

bei den gestiegenen Anforderungen bei der Aufgabenerledigung jedoch heute niemand mehr leisten. Das Angebot von externen Dienstleistern kann zwar gewisse Zwänge mildern. Auf der anderen Seite treten bei manchen Institutionen, die unter einem besonderen Schutz stehende Daten verarbeiten, dann wieder datenschutzrechtliche Probleme auf.

19.1.2 Wachsende Bedeutung von Sicherheitszertifikaten

In der heutigen Zeit streben die Menschen nach einer immer größeren Absicherung in allen Lebensbereichen. Neben vielen gesetzlich vorgeschriebenen Pflichtversicherungen wird für alle möglichen und unmöglichen Dinge Vorsorge getroffen. Ziel einer jeden Vorsorgemaßnahme ist es, sich gegen unvorhergesehene Ereignisse abzusichern, um beim Eintritt einer entsprechenden Katastrophe keinen finanziellen Schaden zu erleiden.

In der automatisierten Datenverarbeitung sieht es meistens etwas anders aus. Liegt das daran, daß die Beteiligten die Risiken vieler evidenten Sicherheitsdefizite nicht erkennen oder daß bisher zu wenig Schäden und IT-Katastrophen auf Sicherheitsdefizite zurückzuführen waren? Oder liegt es einfach daran, daß man nicht dazu in der Lage ist, zu erkennen, welche der angebotenen Sicherheitskomponenten die Sicherheit in der Datenverarbeitung entscheidend verbessern können? Viele Anwender sind bei der Beurteilung der Wirksamkeit dieser Sicherheitseinrichtungen sicherlich überfordert. Sie sind auf das Urteil eines sachverständigen Dritten angewiesen. Bei der Vielfältigkeit heutiger Datenverarbeitungsprozesse und der nahezu unbegrenzten Datenvernetzung ist man auf eine Sicherheitszertifizierung, wie sie vom [BSI](#) (*Link - Neues Fenster*) und den vom BSI akkreditierten Zertifizierungsstellen angeboten wird, mehr denn je angewiesen.

Der Wunsch nach einer Sicherheitszertifizierung von IT-Komponenten tauchte schon in den Anfängen des Datenschutzes auf. So beschäftigte man sich bereits auf einer Sitzung des Beirats beim Bayer. Landesbeauftragten für den Datenschutz Anfang der 80er-Jahre mit diesem Thema. Wohl durch die damaligen US-amerikanischen Bestrebungen ermutigt, forderte man, auch in Deutschland von einer unabhängigen Stelle die Sicherheitsfunktionen in IT-Systemen hinsichtlich ihrer Effektivität und Stärke zertifizieren zu lassen. Zu jener Zeit glaubte man noch, ohne größere Probleme kompletten Anwendungssystemen sog. typgeprüfte Sicherheitsplaketten verleihen zu können, die dem Anwender die Systemauswahl wesentlich erleichtern könnten. Heute, fast 20 Jahre danach, ist man - infolge der rasanten technischen Entwicklung - von einer solchen

Wunschvorstellung noch immer weit entfernt.

Das Szenario stellt sich vielmehr etwa folgendermaßen dar:

- Der Markt wird von einer Unzahl von Hard- und Softwareprodukten überschwemmt, die alle Möglichkeiten, Informationen zu verarbeiten, eröffnen.
- Über das Internet kann man Verbindung zu einer Vielzahl von Rechnern aufnehmen und sich dort Daten beschaffen. Diese Daten werden im eigenen Rechner gespeichert, nach beliebigen Kriterien ausgewertet und mit anderen Daten zu neuen Qualitäten verknüpft.
- Viele Institutionen sind überfordert, wenn sie abschätzen sollen, in welchen Systemen welche Sicherheitslücken enthalten sind oder durch unsachgemäße Handhabung entstehen können.

Die Datenschutzkontrollinstanzen befinden sich in diesem Spannungsfeld; sie sollen Sicherheitsdefizite aufdecken und Lösungsvorschläge entwickeln. Bei dem breiten Spektrum der Produktpalette der verschiedenen Hersteller ist das ein Unterfangen, das eigentlich nur mit zusätzlichen Experten möglich wäre. Diese Experten müßten über leistungsfähige Instrumente und über Verfahrensweisen verfügen, die es ihnen erlauben, die Funktionalität und Qualität von Sicherheitsfunktionen in den IT-Systemen nach einheitlichen, international anerkannten Kriterien (ITSEC oder Common Criteria) zu bewerten, sprich zu zertifizieren. Seit Anfang der 90er-Jahre gibt es mit dem BSI eine solche staatliche Zertifizierungsstelle.

Leider entspricht die Anzahl bisher sicherheitszertifizierter IT-Produkte nicht dem Bedarf, den Anwender und Kontrollinstanzen haben. So erhebt sich die Frage, wo die Gründe für diese Erscheinung zu suchen sind:

- Einmal dürften wohl die beträchtlichen Kosten, die für eine Zertifizierung zu entrichten sind, viele Unternehmen von einem Gang zur Zertifizierungsstelle abschrecken. Zudem erscheint es fraglich, ob sich ein zertifiziertes Produkt besser verkauft als ein nichtzertifiziertes, da es noch keine verbindlichen Vorgaben (ausgenommen in bestimmten besonders sicherheitsrelevanten Bereichen) gibt, ausschließlich zertifizierte Produkte einzusetzen. Auf der anderen Seite wächst das Bewußtsein in der Öffentlichkeit über die datenschutz- und -sicherheitsmäßigen Risiken in der modernen Informationstechnologie.
- Eine weitere Hemmschwelle, ein Produkt zertifizieren zu lassen, dürfte auch in den langen Zertifizierungszeiten liegen. Es ist keine Seltenheit, daß sich Zertifizierungen über Zeiträume hinziehen, die größer als die üblichen Innovationszyklen der Produkte und

länger als die Lebensdauer einer Version sind.

- Schließlich garantiert der Einsatz eines zertifizierten Produktes dem Anwender noch lange nicht die gewünschte Sicherheit. Sie hängt häufig sehr davon ab, unter welchen Rahmenbedingungen ein zertifiziertes Produkt eingesetzt wird. Sogenannte gekapselte Systeme sind äußerst selten anzutreffen.

Um aus diesem Dilemma herauszukommen, müssen unbedingt neue Wege beschritten werden.

Folgende Maßnahmen können dabei helfen:

1. Herabsetzung der Zertifizierungszeiten
2. Senkung der Kosten für eine Zertifizierung
3. Zusammenarbeit aller Zertifizierungsinstanzen mit dem Ziel, Sicherheitszertifikate gegenseitig anzuerkennen
4. Inhouse-Zertifizierung durch potente, vertrauenswürdige Anbieter
5. Entwicklung von Sicherheitsstandards, die sich in Anwendungssysteme problemlos integrieren lassen, so daß diese Anwendungssysteme nicht mehr zertifiziert zu werden brauchen. Als Beispiel wären hier Systeme zur Sicherung der Vertraulichkeit übertragener Informationen anzuführen.
6. Einbeziehung von Services, wie Wartung, Fernwartung oder "outsourcte" Systemdienste in die Zertifizierung.

Viele Anwender stehen heute durch die Aufgabenmehrung unter einem erhöhten Leistungsdruck, der nur mit Hilfe der automatisierten Datenverarbeitung zu bewältigen ist. Sie verfügen jedoch meist nicht über das wünschenswerte Know-how auf dem Gebiet der Systemsicherheit, weil sie personell so spartanisch ausgestattet sind, daß sie sich keine Spezialisten leisten können. Diese Anwender warten geradezu auf Produkte, die von einer vertrauenswürdigen Stelle sicherheitszertifiziert wurden.

Durch die Anerkennung von Sicherheitszertifikaten privater Zertifizierungsstellen durch die amtliche Zertifizierungsbehörde ([BSI \(Link - Neues Fenster\)](#)) wird seit Anfang 1998 ein viel versprechender Weg beschritten, die oben vorgeschlagenen Maßnahmen zeitnah zu realisieren. Es bleibt nur zu hoffen, daß diese positiven Ansätze nicht durch zu hohe Kosten, die auf die Anwender weitergeben werden, im Keime ersticken. Diese Kosten könnten sich kontraproduktiv auf die Bereitschaft, die entsprechenden Schutz- und Vorsorgemaßnahmen zu treffen, auswirken.

19.1.3 Datenschutzfreundliche Technologien

Der zunehmenden Gefährdung der Privatheit des Einzelnen durch die stetig zunehmende Nutzung von IuK-Technik kann nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten wirksam begegnet werden. Den Ansprüchen der Datenschutzfreundlichkeit können IuK-Systeme demzufolge zukünftig nur noch gerecht werden, wenn sie nach dem Prinzip der **Datensparsamkeit** arbeiten. Dabei werden so wenig personenbezogene Daten wie möglich erhoben, gespeichert und verarbeitet. **Datenvermeidung**, d.h. es werden bei der Nutzung von IuK-Systemen keine personenbezogenen Daten erhoben, gespeichert und verarbeitet, ist die stets anzustrebende Form der Datensparsamkeit.

Inhaltlich sind diese Forderungen (siehe schon meine "[Überlegungen zu aktuellen Problemen des Datenschutzes](#)" 1996, S. 16f, einseh- und abrufbar auf meiner Homepage) bereits seit längerem in den Datenschutzgesetzen des Bundes und der Länder durch den Grundsatz der Erforderlichkeit festgelegt. Dieser war auch schon bisher bei der Ausgestaltung der IuK-Technik zu beachten, mit der technischen Entwicklung gewinnt er aber zunehmende Bedeutung. Es ist daher sehr zu begrüßen, daß der Grundsatz der Datenvermeidung nunmehr im Informations- und Kommunikationsdienste-Gesetz ([IuKDG](#)), dort in Art. 2 Teledienstedatenschutzgesetz ([TDDSG](#)), und im Mediendienste-Staatsvertrag ([MDSStV](#)) ausdrücklich enthalten ist. Danach haben Anbieter von Tele- bzw. Mediendiensten den Nutzern die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung eines Pseudonyms zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht erstellt hat, betont in Kapitel 2.5 seiner Entschließung zu der Empfehlung an den Europäischen Rat "Europa und die globale Informationsgesellschaft" und zu der Mitteilung der Kommission "Europas Weg in die Informationsgesellschaft: Ein Aktionsplan" (Deutscher Bundesrat, Drucksache 776/96, 10.10.1996, Bonn) folgendes: "Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern".

Die europäische Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr (Richtlinie 95/46/EG vom 24. Oktober 1995, Amtsblatt Nr. L 281, S. 31) enthält den Grundsatz, daß eine Verarbeitung personenbezogener Daten

nur stattfinden darf, soweit sie im Hinblick auf bestimmte und festgelegte Zwecke notwendig ist. Sie geht deshalb auch von dem Prinzip aus, daß das Recht auf Privatsphäre und Selbstbestimmung dadurch am wirksamsten geschützt wird, daß möglichst keine personenbezogenen Daten erhoben werden. Im Hinblick auf die Umsetzung dieses Grundsatzes fördert die Europäische Kommission die Entwicklung und Anwendung datenschutzfreundlicher Technologien, insbesondere im Rahmen des elektronischen Handels, sowie beispielsweise die Möglichkeit eines anonymen Zugangs zu Netzen und anonyme Zahlungsweisen (Kommissionsvorschlag zum 5. Rahmenprogramm für Forschung und technologische Entwicklung, KOM (97)142 und Mitteilung der Kommission zum elektronischen Handel, KOM (97)157).

In Abschnitt [18.1.6.](#) meines 17. Tätigkeitsberichts habe ich ausgeführt, daß sich der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder mit den Fragen der datenschutzfreundlichen Technologien befaßt und ein entsprechendes Grundsatz- und Arbeitspapier erstellt. Auf der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. und 24. Oktober 1997 in Bamberg haben die Datenschutzbeauftragten den Abschlußbericht des Arbeitskreises zum Thema "[Datenschutzfreundliche Technologien](#)" zustimmend zur Kenntnis genommen.

In dem unter meiner Federführung erstellten Teil I (als Grundsatzbericht) wird

- verdeutlicht, in welchem Umfang die Nutzung moderner Techniken, z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien, umfangreiche elektronische Spuren hinterläßt, durch die Verhaltens- und Verbraucherprofile bis hin zu kompletten Persönlichkeitsbildern gewonnen werden können, und
- ausgeführt, wie und wo sich die Speicherung und Verarbeitung personenbezogener Daten minimieren läßt, z.B. durch Einsatz von kryptografischen Verfahren (Verschlüsselungsverfahren) und der Anwendung von Anonymisierungs- und Pseudonymisierungstechniken. An Hand mehrerer Beispiele wird aufgezeigt, welche Möglichkeiten dazu bestehen, u.a. im Medienbereich, bei elektronischen Zahlungsverfahren, im Gesundheitsbereich und im Bereich Transport und Verkehr.

Der unter Federführung meiner Kollegin aus Nordrhein-Westfalen erstellte Teil II befaßt sich speziell mit "Datenschutzfreundlichen Technologien in der Telekommunikation".

Das Grundsatzpapier "[Datenschutzfreundliche Technologien](#)" steht auf meiner Homepage zum Abruf bereit. Der Vorsitzende des AK Technik hat die gesamte Ausarbeitung in einer Broschüre,

die auch bei meiner Geschäftsstelle angefordert werden kann, herausgegeben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder faßte zu dem Thema "Datenschutzfreundliche Technologien" eine Entschlieung, mit der sie sich sowohl an den Gesetzgeber wie auch an Hersteller und Anbieter von IuK-Systemen wendet und diese auffordert,

- die Verwendung datenschutzfreundlicher Technologien durch entsprechende gesetzliche Rahmenbedingungen zu forcieren und
- bei der Konzeption von IuK-Systemen von vornherein auf eine konsequente Minimierung der Verarbeitung und Speicherung personenbezogener Daten zu achten.

Auerdem fordert die Konferenz in der Entschlieung, da Informations- und Kommunikationssysteme (IuK-Systeme) schon in der Konzeptionsphase durch Einsatz intelligenter Technik und Organisation datenschutzfreundlich gestaltet werden. Der Text der Entschlieung ist diesem Ttigkeitsbericht als Anlage ([Anlage 12](#)) beigelegt.

19.1.4 Einsatz kryptografischer Verfahren

Allgemeines

Auch in diesem Berichtszeitraum wurde mir hufig die Frage gestellt, wie schutzwrdige Daten bei der Speicherung auf Festplatten (z.B. in Laptops und Notebooks), aber ganz besonders bei der bertragung ber Datennetze gegen eine unbefugte Kenntnisnahme und Vernderung geschtzt werden knnen. Insbesondere vor dem Hintergrund der dramatisch zunehmenden internen und auch hausbergreifenden Vernetzung, der Anbindung von Auenstellen an hauseigene DV-Netzwerke und der Einrichtung von Telearbeitspltzen kommen der Sicherstellung der Authentizitt und der Vertraulichkeit der Kommunikationsinhalte sowie der Sicherstellung der Datenintegritt bei einem bertragungsvorgang ber fremde Datenleitungen besondere Bedeutung zu.

Es ist festzustellen, da

- die Datennetze von sich aus keine Sicherheitsmechanismen bereitstellen, mit denen Authentizitt, Integritt und Vertraulichkeit gewhrleistet werden knnen,
- Daten bei Speicherung und bei bertragung nur durch den Benutzer selbst und durch Anwendung geeigneter kryptografischer Verfahren (Verschlsselungstechniken) vor un-

befugter Kenntnisnahme und vor unbefugter Veränderung wirksam geschützt werden können und

- es in der Bundesrepublik Deutschland keine gesetzliche Regelung bzgl des Einsatzes kryptografischer Verfahren gibt, er also zulässig ist.

Kryptodebatte

In der ersten Hälfte des Berichtszeitraums wurde bundesweit eine heftige Diskussion, die sog. Kryptodebatte oder Kryptokontroverse, um ein eventuelles Kryptografiegesetz in der Bundesrepublik geführt.

Dabei ging es um das Für und Wider einer staatlichen Reglementierung des Kryptografieeinsatzes in der Form, daß nur solche kryptografischen Produkte zur Verfügung stehen sollten bzw. verwendet werden dürften, die durch staatliche Stellen bzw. durch staatlich akkreditierte Privateinrichtungen zugelassen sind. Entscheidend dabei wäre auch, daß die verwendeten Schlüssel entweder als Nachschlüssel (Key Escrow) sicher hinterlegt werden müßten oder eine Rekonstruktion der verwendeten Schlüssel möglich wäre (Key Recovery), um unter bestimmten gesetzlichen Bedingungen für Sicherheitsbehörden zugänglich zu sein.

Anläßlich der Eröffnung des 5. IT-Sicherheitskongresses des Bundesamts für Sicherheit in der Informationstechnik am 28. April 1997 in Bonn bezeichnete der Bundesinnenminister die Kryptografie als eine Schlüsseltechnologie für eine sichere Informationsgesellschaft. Er betonte ausdrücklich, daß die Verschlüsselung zum Schutz der Vertraulichkeit eine unverzichtbare Grundvoraussetzung für die Anwendung der Informationstechnik sei. Gleichzeitig hob er jedoch das Bedürfnis und den Anspruch des Staates nach legalen Überwachungsmöglichkeiten durch die Strafverfolgungs- und Sicherheitsbehörden hervor.

Ich sehe die konkurrierenden Zielsetzungen - eine Lösung dieses Dilemmas vermag auch ich nicht zu nennen. Ich vertrete jedoch die in der Debatte genannten Argumente, nämlich daß

- die Kryptografie ein ausgezeichnetes Mittel zur Wahrung der Privatheit des Einzelnen, zur Wahrung des informationellen Selbstbestimmungsrechts und damit zur Sicherung des Datenschutzes ist,
- ein Kryptoverbot oder eine Kryptoeinschränkung die Zielrichtung nach Kriminalitätsbekämpfung verfehlen würde, weil sie praktisch nicht durchsetzbar wären und
- eine Schlüsselhinterlegung ebenso wie Methoden zur Schlüsselwiedergewinnung abzulehnen sind, weil dadurch zusätzliche Risiken für die Wahrung der Vertraulichkeit, der

Authentizität und der Integrität entstünden und solche Maßnahmen den sicherheitsphilosophischen Grundaspekten der Public-Key-Systeme (Privater Schlüssel, Öffentlicher Schlüssel) zuwiderlaufen und diese insgesamt in Frage stellen würden.

Auch die Enquete-Kommission des Deutschen Bundestages "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft" kommt in ihrem Vierten Zwischenbericht zum Thema Sicherheit und Schutz im Netz (Drucksache 13/11002, 22.06.1998, Bonn, S. 69) vom 22.06.1998 zu den gleichen Ansichten. Im übrigen vertritt die Kommission die Auffassung, daß "alle Maßnahmen und Hemmnisse, die einer breiten Nutzung von Verschlüsselungsverfahren entgegenwirken, vermieden und abgebaut werden müssen. Darüber hinaus sollte die breite Nutzung kryptografischer Verschlüsselungsmethoden aktiv unterstützt und gefördert werden. In diesem Zusammenhang sind Bund und Länder aufgefordert, geeignete Verschlüsselungsmethoden systematisch in ihrem elektronischen Datenverkehr einzusetzen." Diese Einschätzung macht die Kommission in ihrem Schlußbericht zum Thema Deutschlands Weg in die Informationsgesellschaft (Drucksache 13/11004, 22.06.98, Bonn, S. 14 ff.) vom 22.06.98 noch deutlicher, in dem sie schreibt: "... Eine Beschränkung des Gebrauchs von Verschlüsselungstechniken ist nach derzeitigem Erkenntnisstand daher abzulehnen." Außerdem hebt die Kommission hervor, daß "...IT-Sicherheit nicht nur als Kostenfaktor dargestellt werden" sollte, sondern "vielmehr ... als Leistungsmerkmal von IT-Systemen und ... als Wettbewerbsfaktor ..." gesehen werden sollte. Beide Berichte sind im Internet unter der Adresse "<http://www.bundestag.de/gremien/enquete/14344x.htm>" (*Link - Neues Fenster*) verfügbar. In diesem Zusammenhang sei auch auf das Papier "[Datenschutzfreundliche Technologien](#)" des AK Technik verwiesen.

Die Debatte ist derzeit etwas abgeflaut, sie ist aber noch nicht abgeschlossen.

Praktische Anwendungsformen

Im Abschnitt [18.1.4](#) meines 17. Tätigkeitsberichts von 1996 bin ich auf die verschiedenen Formen der Verschlüsselungstechniken (symmetrische Verschlüsselung, asymmetrische Verschlüsselung, hybride Verschlüsselung) eingegangen und habe deren Funktionsweisen und Unterschiede näher beschrieben.

In der Praxis kann der Einsatz kryptografischer Verfahren auf zwei grundlegend verschiedene Arten erfolgen:

- Werden die Daten permanent verschlüsselt im DV-System gespeichert, so entfällt der Bedarf für eine Verschlüsselung speziell für Übertragungszwecke und die Daten können grundsätzlich ohne weiteres übertragen werden. Dieses Vorgehen ist bei besonders schutzwürdigen Daten zu empfehlen.
- Werden die Daten erst und nur für die Übertragung verschlüsselt, so kann der Verschlüsselungsvorgang
 - einerseits bewußt durch den Anwender oder
 - andererseits automatisch durch entsprechende Software, durch Zusatzgeräte (Kryptoprozessor, Kryptierkarte, Kryptierbox) oder durch Netzkopplungselemente (Netzkarten, Router)

durchgeführt werden. Die bewußt durch den Anwender angestoßene Verschlüsselung ermöglicht zwar eine Differenzierung nach Schutzwürdigkeit der zu übertragenen Daten, birgt aber die Gefahren der Fehlentscheidung und des Vergessens. Die automatisch angestoßene Verschlüsselung bietet insoweit eine höhere Zuverlässigkeit und dürfte auch als anwenderfreundlicher betrachtet werden. In der Regel kann auch davon ausgegangen werden, daß Verschlüsselungshardware weniger Rechnerleistung verbraucht und schneller, aber teurer als Verschlüsselungssoftware ist.

Grundsätzlich gilt natürlich, daß der Einsatz von Kryptografieprodukten i.d.R. bei allen Kommunikationspartnern die gleiche bzw. eine kompatible Ausstattung bzgl. dieser Kryptografieprodukte bedingt. Es gibt mittlerweile aber auch Lösungen, die durch entsprechende Voreinstellungen sowohl eine verschlüsselte Kommunikation mit vordefinierten Partnern als auch eine unverschlüsselte Kommunikation mit anderen Partnern ermöglichen. Gerade solche Lösungen erscheinen für die Verwendung in Netzwerken der öffentlichen Verwaltung, die auch Kommuni-

kation z.B. mit Bürgern betreiben wollen, besonders geeignet.

Die am weitest verbreiteten und in entsprechender Software bzw. Hardware verwendeten Verschlüsselungsalgorithmen stammen derzeit noch aus den USA. Diese Implementierungen verwenden aber einerseits kleine Schlüssellängen, die keine hinreichende Sicherheit mehr bieten, und andererseits unterliegt der Auslandsvertrieb dieser Produkte mit größeren und damit hinreichenden Schlüssellängen strengen US-Exportrestriktionen. Ausnahmegenehmigungen wurden und werden allerdings nur erteilt für bestimmte Branchen bzw. wenn entsprechende Key Recovery-Mechanismen durch den Hersteller dem zuständigen US-Wirtschaftsministerium zur Verfügung gestellt werden.

Wie oben dargestellt, lehne ich derartige Key Recovery Methoden ab. Aber auch wenn die vorhandenen Werkzeuge bekanntermaßen Schwachstellen aufweisen, so möchte ich deutlich darauf hinweisen, daß deren derzeitige Nutzung immer noch besser ist als überhaupt keine Schutzmechanismen einzusetzen.

Erfreulich ist in diesem Zusammenhang, daß eine Reihe von Behörden und Einrichtungen Bayerns bereits von sich aus dies erkannt und trotz der zusätzlichen Kosten nach für ihre Bedürfnisse geeigneten Lösungen suchen und gesucht haben und z.T. bereits einsetzen.

Zunehmend stehen auf dem Markt auch deutsche und europäische Kryptografieprodukte sowohl auf Hardware- als auch auf Softwarebasis zu erschwinglichen Preisen und für alle möglichen Anforderungen zur Verfügung. Es sind auch Kryptografieprodukte erwerbbar, deren Leistungsumfang sich nicht nur auf die Verschlüsselung von Daten beschränkt, sondern mit denen auch digitale Signaturen angefertigt und die in Kombination mit Chipkarten (als starkem Authentifizierungshilfsmittel und ggf. sicherem Speicher der elektronischen Schlüssel) verwendet werden können. In diesem Zusammenhang sei auf das Projekt BASILIKA im Rahmen von Bayern Online ([Nr. 19.3.1](#)) hingewiesen.

Digitale Signaturen

Neben dem oben dargestellten Schutzziel der Vertraulichkeit sind die Schutzziele der Integrität und der Authentizität bei einer Datenübertragung über offene Netze von besonderer Bedeutung, d.h.

- zu gewährleisten, daß der Empfänger die vom Absender übermittelte Information unverändert erhält bzw. unzulässige Veränderungen zumindest erkennen kann;
- zuverlässig erkennen zu können, daß eine Information auch tatsächlich von dem angegebenen Absender stammt;
- bei Bedarf eine Garantie zu erhalten, daß jemand eine bestimmte Nachricht tatsächlich verfaßt, versandt bzw. erhalten hat (Unabstreitbarkeit).

Diesen Aspekten wird mit dem Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - [IuKDG](#)) vom 13. Juni 1997 und hier speziell mit dem Artikel 3, Gesetz zur digitalen Signatur (Signaturgesetz - [SigG](#)), sowie der dazu erlassenen Verordnung zur digitalen Signatur (Signaturverordnung - [SigV](#)) vom 22. Oktober 1997 Rechnung getragen. Zweck des Signaturgesetzes ist, "Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können." ([§ 1 Abs. 1 SigG](#)).

Digitale Signaturen basieren auf dem Konzept der Public-Key-Kryptosysteme. Hierbei verfügt jeder Benutzer über ein Schlüsselpaar, bestehend aus einem nur ihm bekannten Privaten Schlüssel und einem publizierten Öffentlichen Schlüssel. Zur Signierung eines digitalen Dokuments wird zunächst über komplexe mathematische Verfahren (sog. Hashverfahren) aus dem zu signierenden Dokument ein Wert fester Länge (sog. Hashwert) errechnet. Dieser Hashwert wird sodann mittels des Privaten Schlüssels und eines Signaturverfahrens verschlüsselt und dem Dokument angefügt. Dies bedeutet, daß die digitale Signatur eines Benutzers für jedes zu signierende Dokument separat berechnet wird und demzufolge bei zwei verschiedenen Dokumenten im Ergebnis auch unterschiedlich aussieht.

Der Empfänger des signierten Dokumentes kann nun unter Anwendung des gleichen Signaturverfahrens mit dem Öffentlichen Schlüssel des Absenders den verschlüsselten Hashwert des Dokuments entschlüsseln. Stimmt der entschlüsselte Hashwert mit dem durch den Empfänger aus dem übersandten Dokument ermittelten Hashwert überein, so kann der Empfänger sicher sein,

daß das Dokument unverändert übermittelt wurde und daß das Dokument vom Inhaber des Privaten Schlüssels, der zu dem ihm bekannten Öffentlichen Schlüssel gehört, stammt. Ergibt dieser Vergleich keine Übereinstimmung, so wurde das Dokument während des Transports entweder verändert oder es stammt nicht von dem angenommenen Absender.

Es ist damit aber für den Empfänger einer Nachricht noch nicht zweifelsfrei nachgewiesen, daß das Schlüsselpaar auch wirklich zu dem angenommenen Absender gehört. Diese Unsicherheit zu beseitigen, ist ein Ziel des Signaturgesetzes.

Aus technischer Sicht hängt die Sicherheit einer digitalen Signatur primär von der Stärke der zugrunde liegenden Kryptoalgorithmen und der Umgebung ab, in der das Schlüsselpaar, Öffentlicher und zugehöriger Privater Schlüssel, erzeugt und angewendet werden. Das Signaturgesetz, die Signaturverordnung und die zugehörigen Bekanntmachungen tragen diesen Aspekten durch die Vorgaben Rechnung, daß

- eine digitale Signatur auf asymmetrischen Kryptoverfahren (Public Key-Systemen) basiert,
- diese Kryptoverfahren bestimmte Kriterien erfüllen müssen (siehe Bekanntmachung der Regulierungsbehörde für Telekommunikation und Post zur digitalen Signatur nach Signaturgesetz und Signaturverordnung vom 09.02.1998, Bundesanzeiger Nr. 31, 14.02.98),
- nur zertifizierte technische Einrichtungen zur Erzeugung des Schlüsselpaares angewendet und
- nur zertifizierte technische Einrichtungen zur Speicherung und Anwendung des Privaten Schlüssels verwendet werden dürfen.

Die Prüfung der technischen Komponenten hat dabei nach den "Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik" zu erfolgen.

Aus organisatorischer Sicht hängt die Sicherheit einer digitalen Signatur davon ab, wie zuverlässig die Zuordnung Benutzer und Privater Schlüssel erfolgt und wie sorgfältig der Benutzer mit seinem Privaten Schlüssel umgeht. Hinsichtlich dieser Aspekte bestimmen das Signaturgesetz und die Signaturverordnung eine IT-Sicherheitsinfrastruktur, die aus

- der Regulierungsbehörde für Telekommunikation und Post (RegTP),
- Zertifizierungsstellen,
- anerkannten Prüfstellen und

- dem Antragsteller (Teilnehmer)

besteht. Ein Hauptelement in dieser IT-Sicherheitsinfrastruktur ist eine zweistufige Zertifizierungsstruktur mit einer nationalen Wurzelzertifizierungsstelle. Auch die Aufgaben der einzelnen Komponenten der IT-Sicherheitsinfrastruktur sind festgelegt.

So haben die Zertifizierungsstellen, in der Literatur auch häufig Trust Center, Vertrauensstellen, Trusted Third Parties (TTP) und Certification Authorities (CA) genannt, gem. Signaturgesetz und Signaturverordnung folgende Aufgaben:

- zweifelsfreie Identifikation und Registrierung eines Antragstellers
- ggf. Erzeugung des Schlüsselpaares für den Antragsteller
- ggf. Ausgabe der Schlüssel an den Antragsteller
- Zuordnung eines Öffentlichen Schlüssels zu einer Person (Personalisierung und ggf. Pseudonymisierung)
- Zertifizierung des Öffentlichen Schlüssels
- Betrieb und Pflege von öffentlichen Schlüsselverzeichnissen
- Sperrung von Zertifikaten
- Versehen digitaler Daten mit einem Zeitstempel

Ein vom Antragsteller selbst erzeugter Öffentlicher Schlüssel kann auch durch eine Zertifizierungsstelle i.S.d. Signaturgesetzes zertifiziert werden, allerdings nur dann, wenn der Antragsteller zur Erzeugung des Schlüsselpaares sowie zur Speicherung und Anwendung des Privaten Schlüssels zertifizierte technische Komponenten verwendet. Für einen privaten Antragsteller dürfte dies eher die Ausnahme sein.

Durch die zweifelsfreie Identifizierung und Registrierung eines Antragstellers sowie durch die Zertifizierung des zugehörigen Öffentlichen Schlüssels, d.h. digitale Signierung des Öffentlichen Schlüssels durch die Zertifizierungsstelle, wird es für einen Dritten zweifelsfrei möglich, die Authentizität einer digitalen Signatur und damit einer signierten Nachricht festzustellen.

Der Sachstand bei der Umsetzung des Signaturgesetzes (zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht)

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hat am 01.01.1998 ihre Arbeit aufgenommen.

Als Prüfstellen wurden von der Regulierungsbehörde bereits einige Stellen

- für die Bestätigung von technischen Komponenten (§ 17 Abs. 4 SigV und [§ 14 Abs. 4 SigG](#)),
- für die Prüfung und Bestätigung der Umsetzung von Sicherheitskonzepten ([§ 4 Abs. 3 Satz 3 SigG](#)) und
- für die Prüfung der Sicherheit von technischen Komponenten ([§ 14 Abs. 4 SigG](#) und § 17 Abs. 1 SigV)

anerkannt bzw. vorläufig anerkannt. Die Liste der anerkannten und vorläufig anerkannten Prüfstellen ist im Bundesanzeiger veröffentlicht und steht auf der Homepage der Regulierungsbehörde unter der Adresse "<http://www.regtp.de>" (*Link - Neues Fenster*) zum Abruf bereit.

Die erforderlichen Maßnahmenkataloge (mit Stand jeweils zum 15.07.1998) für Zertifizierungsstellen (§ 12 Abs. 2 SigV) und für technische Komponenten (§ 16 Abs. 6 SigV) sind mittels der Bekanntmachung vom 14. September 1998 im Bundesanzeiger veröffentlicht und stehen ebenfalls auf der Homepage der Regulierungsbehörde zum Abruf bereit.

Eine Reihe von Unternehmen haben die Zulassung als Zertifizierungsstelle beantragt. Man rechnet damit, daß Ende 1998 die ersten Zulassungen gem. Signaturgesetz erfolgen. Wann die entsprechenden technischen Komponenten auf dem Markt zur Verfügung stehen werden, läßt sich schwer vorhersagen.

Zusammenfassend bedeutet dies, daß eine digitale Signatur nach dem Signaturgesetz erst bei Vorliegen von Zertifizierungsstellen und von zertifizierten technischen Komponenten realisierbar ist. Über diesen Zeitpunkt können keine Angaben gemacht werden.

Entgegen häufig anzutreffenden Meinungen ist mit dem Signaturgesetz die digitale Signatur der handschriftlichen Unterschrift nicht gleichgestellt. Es gilt lediglich die Sicherheitsvermutung der zertifizierten digitalen Signatur nach [§ 1 Abs. 1 SigG](#). Um das Ziel der rechtlichen Gleichstellung mit der Schriftform des § 126 BGB zu erreichen, müßten noch erhebliche Anstrengungen durch den Gesetzgeber unternommen werden, wie auch aus dem Vierten Zwischenbericht der Enquete-Kommission des Deutschen Bundestages "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft" zum Thema Sicherheit und Schutz im Netz (Drucksache 13/11002, 22.06.1998, Bonn, S. 61) vom 22.06.1998 hervorgeht: "... Mindestens 3907 Regelungen in 908 rechtlichen Vorschriften verlangen heute die Schriftform mit eigenhändiger Unterschrift auf einer Papierurkunde. ..."

Vor dem Ziel, ggf. Verwaltungshandlungen (Anträge, Bescheide, usw.) auch elektronisch abwickeln zu können, ist dies noch eine beträchtliche Einschränkung bzgl. Rechtsgültigkeit und Verbindlichkeit und damit der Nutzbarkeit von digitalen Signaturen auch im Bereich der öffentlichen Verwaltung. In diesem Zusammenhang verweise ich auf den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen (KOM(1998) 297 endg., Brüssel) vom 13.05.1998. Nach Art. 5 dieses Richtlinienvorschlages soll die digitale Signatur Rechtsgültigkeit haben und auch, bei Vorliegen entsprechender Voraussetzungen, einer handschriftlichen Unterschrift gleichgestellt und vor Gericht als Beweismittel zugelassen werden.

Nach [§ 1 Abs. 2 SigG](#) ist die Anwendung anderer Verfahren für digitale Signaturen freigestellt. Eine Sicherheitsvermutung wie nach [§ 1 Abs. 1 SigG](#) im Sinne einer Beweiserleichterung im Wege eines vorweggenommenen Anscheinsbeweises bei einer Streitigkeit vor Gericht ist bei Nutzung derartiger Verfahren aber nicht gegeben. Verfahren zur Erzeugung von digitalen Signaturen sind hinlänglich bekannt, erprobt und verfügbar. Als ein Beispiel sei hier nur das aus dem Internet bekannte Pretty Good Privacy (PGP) genannt. Es gibt auch bereits Verfahren und Systeme, die auf Chipkartenbasis operieren, d.h. bei denen eine Chipkarte als Träger des Privaten Schlüssels und gleichzeitig als starkes Authentifizierungsmerkmal ("Wissen und Besitz") fungiert.

Durch kommerziell betriebene Trust Center besteht auch seit geraumer Zeit die Möglichkeit, digitale Signaturen zertifizieren zu lassen; allerdings nicht mit der gesetzlichen Beweiserleichterungswirkung des [§ 1 Abs. 1 SigG](#), da es sich bei einer solchen Zertifizierung - jedenfalls derzeit - nicht um eine solche nach dem Signaturgesetz handelt. Gerade geschlossene Kommunikationsgruppen (z.B. Verwaltungsbereiche) können so, zumindest übergangsweise, entweder eine vorhandene Zertifizierungsinfrastruktur nutzen oder sie könnten auch alternativ eine eigene Zertifizierungsinfrastruktur aufbauen und damit einen erheblichen Zugewinn an Sicherheit in ihrer Kommunikation erlangen (siehe hierzu auch den Abschnitt [Nr. 19.3.1](#), Bayern Online - Sicherheitsarchitektur BASILIKA).

Der mindestens ebenso bedeutsame Aspekt der Vertraulichkeit in offenen Netzen wird durch das [IuKDG](#) leider nicht berührt. Bezüglich der Vertraulichkeit obliegt es dem Benutzer der IuK-Technik nach wie vor selbst, geeignete Maßnahmen zu ergreifen, zumal auch die benutzten Netzwerke i.d.R. keine diesbezüglichen Funktionalitäten bereitstellen.

Die meisten verfügbaren Publik-Key-Verfahren bieten jedoch neben der Funktionalität zur Erzeugung digitaler Signaturen auch eine Option zur Verschlüsselung der Daten, so daß bei Nutzung dieser Funktionalität auch dem Aspekt der Vertraulichkeit Rechnung getragen werden kann.

Praxisbeispiel: Speicherung sensibler Daten auf PC

Im März 1998 erschienen Presseberichte zu einem Vorfall im Thüringischen Innenministerium, bei dem ein Personal Computer, auf dem besonders schutzwürdige Daten gespeichert waren, abhanden gekommen war. In Schreiben an die bayerischen Ministerien und die Bayerische Staatskanzlei habe ich daher insbesondere auf folgende Aspekte hingewiesen:

- Besonders schutzwürdige Daten sollten nur auf zentralen Servern bzw. Zentralrechnern und nicht auf lokalen Festplatten von Personal Computern (PC) gespeichert werden.
- Sollen oder müssen im Ausnahmefall besonders schutzwürdige Daten dennoch lokal auf PC gespeichert werden, so sollten diese Daten, die betreffenden Verzeichnisse oder die ganze Festplatte verschlüsselt werden.
- Die Verwendung von Wechsel-Festplatten, die vom PC getrennt zugriffssicher aufbewahrt und nur bei Bedarf in den PC eingebracht werden können, ist ebenfalls angeraten.

Diese Forderungen möchte ich an dieser Stelle erneut herausstellen und auch darauf hinweisen, daß sie in ganz besonderer Weise für mobile Geräte (Laptops, Notebooks, usw.) gelten.

19.1.5 Sicherheitsaspekte bei der Nutzung des Internets

Datenspuren

Wie die "Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" der Europäischen Kommission in ihrer Empfehlung 3/97 feststellt, sind sich die meisten Internet-Benutzer über die durch ihre Online-Tätigkeit für ihre Privatsphäre entstehenden Risiken jedoch nicht bewußt. Insbesondere nicht darüber, daß mit jeder Nutzung des Internet umfangreiche Datenspuren hinterlassen werden.

Erfolgt der Zugang zum Internet aus einem mit einem Firewall-System und Proxy-Diensten abgesicherten Netzwerk heraus, so fallen je nach Konfiguration dieses Firewall-Systems dort eine Vielzahl an rechnerbezogenen Protokollierungsdaten an. Dies ist normalerweise der Fall bei lo-

kalen Netzwerken und bei Inanspruchnahme eines Providers. Ist der benutzte Personal Computer einer bestimmten Person zuordenbar, so sind diese Daten personenbezogen und eventuelle Auswertungen dieser Protokolldaten haben sich an der strikten Zweckbindung zu orientieren und auf die Mitbestimmungsrechte der Personalvertretung wird hingewiesen. Im Internet selbst tritt bei einer derartigen Konstruktion nur die Rechneradresse des Proxy-Servers auf.

Die Erfassung persönlicher Online-Daten kann somit erfolgen durch

- eigene Firewall-Systeme;
- Provider, die Zugangs- und Verbindungsdaten zu Abrechnungszwecken speichern - teilweise erfolgt dies im Ausland und ist dem Geltungsbereich des deutschen Rechts entzogen;
- Logfiles auf den besuchten Zielrechnern im Internet;
- unbemerkte Datenübertragung durch die verwendete Browser-Software vom eigenen zum Zielrechner im Internet (Cookie-Problematik);
- Überwachungsprogramme auf Zielrechnern im Internet, die so persönliche Nutzungsprofile erstellen, sofern die persönlichen Daten des Nutzers bekannt sind oder ermittelt werden können;
- Index-Suchmaschinen über Newsgroups, um so z.B. alle Beiträge einer Person zu finden;
- leichtfertige und auch bewußte Preisgabe eigener persönlicher Daten, die dann mit ursprünglich einem bestimmten Benutzer nicht zuordenbaren Daten verknüpft werden können.

Dadurch entstehen Risiken für das informationelle Selbstbestimmungsrecht in Form

- der Schaffung von Möglichkeiten der Überwachung, in dem personenbezogene Daten ohne Einwilligung des Nutzers preisgegeben und Kommunikationsvorgänge überwacht werden können,
- der Profilbildung durch Verknüpfung der anfallenden Datenspuren und
- der Intransparenz der Datenerhebung und -verarbeitung für den Betroffenen.

Systemdatenschutz

Vom Internet selbst werden nur wenige Sicherheits- und Schutzmechanismen bereitgestellt. Dies liegt am derzeit verwendeten IP Protokoll der Version 4 und natürlich an der Grundkonzeption des Internet an sich, das zunächst nur für die freie und offene wissenschaftliche Kommunikation gedacht war. Hinzu kommen die Schwächen, Lücken und Fehler in den nutzbaren Diensten. Da Datenpakete im Prinzip von jedermann auf der Übertragungsstrecke ausgewertet werden können, lassen sich unter Ausnutzung dieser Schwächen übertragene Daten (Benutzerkennungen, Paßwörter, sonstige schutzwürdige Daten) mitlesen, verändern, erweitern, fehlleiten oder vernichten und ggf. für weitere Angriffe verwenden.

Sinnvollerweise sollten bereits von den Netzen und der IuK-Technik selbst, wie im Abschnitt "Datenschutzfreundliche Technologien" ausgeführt, Mechanismen bereitgestellt werden, die zumindest die Authentizität und Vertraulichkeit der übertragenen Daten sicherstellen. Vor diesem Hintergrund sind die Bemühungen nach einer Verbesserung des IP Protokolls in Form der Version 6 (IPv6, IPng) zu sehen. Nähere Informationen können z.B. bei der Universität Münster unter der Internet-Adresse "<http://www.join.uni-muenster.de>" (*Link - Neues Fenster*) abgerufen werden. Wann IPv6 allerdings realisiert und flächendeckend umgesetzt sein wird, ist derzeit nicht erkennbar.

Selbstdatenschutz

Da die vom Internet bereitgestellten Mechanismen nicht ausreichen, muß der Benutzer selbst entsprechende Maßnahmen ergreifen, um sich und seine Daten zu schützen. Das sind beispielsweise:

- Zurückhaltung bei der Weitergabe von persönlichen Daten wie E-Mail-Adresse, Name, Anschrift, Telefonnummer usw.
- Zurückhaltung, wenn die anzugebenden Daten für den Zweck der gewünschten Dienstleistung überzogen oder unnötig erscheinen
- Verwendung neuer Browser-Versionen (nach angemessener Zeit) und Nutzung der darin enthaltenen Schutz- und Warnmechanismen
- Nutzung verfügbarer kryptografischer Methoden und Techniken wie
 - digitale Signatur
 - Datenverschlüsselung

- zertifizierte Web-Server
- sichere Protokolle und Technologien (z.B. SSL, S/MIME)
- Soweit möglich anonyme bzw. pseudonyme Nutzung des Internet, z.B. durch Nutzung von Anonymisierungsservern und "Remailern", die einen pseudonymen Versand von E-Mail ermöglichen
- Löschung der Cookie-Dateien unmittelbar nach Ende einer Internet-Sitzung oder zumindest Benutzung der im verwendeten Browser evtl. vorhandenen Option, bei Anlegen eines Cookies eine Meldung am Bildschirm auszugeben
- Nutzung der im verwendeten Browser evtl. vorhandenen Optionen zur Sicherheitseinstellung bzgl. ActiveX und JAVA-Applets ggf. bis dahin, eine Ausführung derartiger Komponenten nicht zuzulassen.

Es sei auch auf die von der spanischen Datenschutzkommission herausgegebenen Empfehlungen für Internet-Benutzer (<http://www.ag-protecciondatos.es> (*Link - Neues Fenster*)), die Feststellungen im Vierten Zwischenbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft des Deutschen Bundestages zum Thema Sicherheit und Schutz im Netz vom 22. Juni 1998 sowie auf den Entwurf der Richtlinien für den Datenschutz im Internet der Projektgruppe zum Datenschutz (CJ-PD) des Europarats vom 13. Mai 1998 (<http://www.coe.fr/dataprotection> (*Link - Neues Fenster*)) hingewiesen.

Technischer Datenschutz

Bereits in meinem letzten Tätigkeitsbericht habe ich in Abschnitt [18.1.1](#) grundsätzliche Forderungen bzgl. notwendiger Basissicherheitsmaßnahmen für den technischen Datenschutz erhoben. An dieser Stelle sei auch nochmals auf die Orientierungshilfe des AK Technik zu "[Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet](#)" hingewiesen, die auch auf meiner Homepage abrufbar ist.

19.2 Prüfungstätigkeit

19.2.1 Kontrolle und Beratungen

Die Kontrolle der technischen und organisatorischen Datensicherheitsmaßnahmen war erneut einer der Schwerpunkte im Berichtszeitraum.

Folgende Dienststellen habe ich nach [Art. 7 BayDSG](#) (teilweise in Verbindung mit [§ 9 BDSG](#) und Anlage) im Berichtszeitraum kontrolliert:

- AOK-Datenannahme und Verteilungsstelle (DAV)
- AOK-Dienstleistungszentrum Regensburg
- AOK-Rechenzentrum Nordbayern
- Bayer. Staatsministerium für Ernährung, Landwirtschaft und Forsten (Landwirtschaftsrechenzentrum)
- Bayerisches Rotes Kreuz (Rettungsleitstelle Passau)
- Fachhochschule Würzburg-Aschaffenburg-Schweinfurt
- Flüchtlingsamt München
- Gemeinde Bayrischzell
- Gemeinde Seefeld
- Landesversicherungsanstalt Oberfranken und Mittelfranken
- Landkrankenhaus Coburg
- Landratsamt Cham
- Landratsamt Freyung-Grafenau
- Landratsamt Passau
- Registerstelle des Epidemiologischen Krebsregisters in Bayern
- Staatliches Schulamt Weissenburg-Gunzenhausen
- Staatsanwaltschaft beim Landgericht Fürth
- Stadt Coburg
- Städtisches Krankenhaus München-Bogenhausen
- Städtisches Krankenhaus München-Harlaching
- Städtisches Krankenhaus München-Neuperlach
- Tumordokumentationsstelle des Klinikums der Universität Regensburg

- Tumorregister im Zentralklinikum Augsburg
- Tumorzentrum der Universität Erlangen-Nürnberg
- Tumorzentrum der Universität Würzburg
- Vertrauensstelle des Epidemiologischen Krebsregisters in Bayern

Die Prüfungen bei den städtischen Krankenhäusern in München betrafen hauptsächlich die Datensicherheitsmaßnahmen im Krankenhausinformationssystem SAP R/3.

Beim Landratsamt Cham wurden insbesondere die für das Bürger- und Kommunale Behördennetz getroffenen technischen und organisatorischen Maßnahmen des Datenschutzes geprüft. Zusätzlich habe ich wieder zahlreiche Dienststellen hinsichtlich der Datensicherheit beraten, wobei vor allem die Gefahren bei einer Öffnung der lokalen Netze nach außen (insbesondere bei einem Internetanschluß) und die dabei zu ergreifenden Sicherheitsmaßnahmen im zunehmenden Maße Gegenstand der Beratungen waren. Auch bei der Entwicklung geeigneter Notfallkonzepte für die lokalen Netze wird meine Geschäftsstelle immer häufiger beteiligt.

19.2.2 Ergebnisse der Kontrolltätigkeit

Die weiterhin angespannte Haushaltslage zwingt viele Dienststellen zum Sparen. Trotzdem bemühten sich die meisten kontrollierten Dienststellen, den Datenschutz und die Datensicherheit zu gewährleisten. So konnte ich einigen Dienststellen bescheinigen, daß die Datensicherheit nahezu vorbildlich gewährleistet ist. Allerdings mußte ich auch in diesem Berichtszeitraum wieder einige schwerwiegende Mängel feststellen. Auf einige möchte ich etwas ausführlicher eingehen:

Verschlüsselung bei der Datenfernübertragung

Sensible personenbezogene Daten, die über öffentliche Leitungen und für jedermann zugängliche Netze übertragen werden, müssen verschlüsselt werden, da die Vertraulichkeit der Informationen sonst nicht gewährleistet ist und die Daten für mißbräuchliche Zwecke aufgezeichnet und verwendet werden könnten. Dies gilt auch für das Behördennetz, da auch hier die Vertraulichkeit der Informationen in den Knotenrechnern des Netzbetreibers oder eventueller Subunternehmer nicht gewährleistet ist. Es gibt eine Reihe von wirksamen Kryptoverfahren, die sich dafür eignen. Insbesondere sollte der Einsatz von Hardwarekomponenten bedacht werden.

Reaktion des Systems auf Fehlversuche

Nach mehrmaliger (höchstens fünfmaliger) mißbräuchlicher oder ungültiger Anmeldung im Netzwerk in ununterbrochener Reihenfolge muß bei allen Clients der Anmeldedialog abgebrochen und das entsprechende Endgerät "out of service" gesetzt bzw. die betreffende Benutzerkennung gesperrt werden. Den Ursachen für fehlerhafte Anmeldeversuche ist nachzugehen, damit Vorsorge gegen etwaige Wiederholungsfälle getroffen werden kann.

Entsorgung von Festplatten

Für die Wartung von Festplatten außer Haus müssen zusätzliche Regelungen getroffen werden, in denen die erforderlichen Sicherheitsmaßnahmen (z. B. physikalisches Löschen der Daten bzw. Vernichtung der Datenträger) beschrieben sind. Auch die Einschaltung von Subunternehmern und die Weitergabe der Datenträger ins Ausland (ob überhaupt und gegebenenfalls unter welchen Bedingungen) müssen geregelt werden.

Katastrophenvorsorge

Jede datenverarbeitende Stelle (unabhängig von ihrer Größe) muß ein detailliertes Backup-Konzept in Form eines Notfallhandbuches für den Katastrophenfall erstellen, damit die Dauer des Ausfalls der EDV bei einem Notfall minimalisiert wird. Insbesondere sollte die Trennung der zentralen Netzverteilung von den Rechnern (Servern) und die Aufstellung von Ersatzservern in einem eigenen Brandabschnitt bedacht werden.

Ich möchte auch auf die in den vorherigen Tätigkeitsberichten aufgeführten Maßnahmen zur Mängelbeseitigung (z. B. Absicherung von Server- und Netzverteilungsräumen, revisionsfähige Dokumentation der Zugriffsberechtigungen, Paßwortvergabe und -änderung durch den Anwender, Protokollauswertung, Deaktivierung von Modems außerhalb der Benutzung, Bestellung und Einbindung eines internen Datenschutzbeauftragten, Führen eines Anlagen- und Verfahrenszeichnisses) hinweisen, weil diese noch nicht in dem gebotenen Maße bekannt sind.

19.3 Technische Einzelfragen

19.3.1 Bayern Online

Die Bayerische Staatsregierung fördert seit 1995 aus Privatisierungserlösen im Rahmen des Projektes "Bayern Online" eine Reihe von Telekommunikationsvorhaben. Diese Initiative hat mit ihren Pilotprojekten dazu beitragen, daß moderne Telekommunikationstechnologien in Bayern sowohl der Bevölkerung als auch der Privatwirtschaft und öffentlichen Verwaltung frühzeitig zugänglich wurden. Die Grundlage dafür war die Schaffung eines Telekommunikationsnetzes, das hohe Datenübertragungsraten zuläßt. Durch Ausbau und Erweiterung des bayerischen Hochschulnetzes, das alle 25 bayerischen Hochschulstandorte miteinander verbindet, konnte das erreicht werden.

Bei einem derartigen Netz, das vielen Benutzern auch den Zugang zum Internet ermöglicht, handelt es sich um ein offenes Netz. Der Anschluß von internen Netzen erfordert deshalb eine Reihe von Sicherheitsmaßnahmen, die sowohl eine vertrauliche und verbindliche Kommunikation zulassen als auch die internen Netze gegen unbefugte Eindringlinge abschotten. Bayern Online fördert auch dafür einige Projekte (Health Care Professional Protocol (Telemedizin), BASILIKA), deren Implementierung Voraussetzung dafür ist, daß auch in einem offenen Netz eine vertrauliche Kommunikation möglich ist. Eine Kürzung der Fördermittel für diese Projekte, wie sie von Seiten des Staatsministeriums der Finanzen beabsichtigt ist, halte ich deshalb für unvertretbar.

Sicherheit im Bayerischen Behördennetz (BYBN)

Das aufgrund der Ministerratsbeschlüsse vom 05.03. und 07.05.1996 aufgebaute Bayerische Behördennetz (BYBN) für die Dienststellen des Freistaats Bayern wird derzeit von dem auch für Bayern Online ausgewählten Provider betrieben. Für den Raum München gibt es ein vom Landesamt für Statistik und Datenverarbeitung (LfStaD) betriebenes Teilnetz (Kernnetz), das in das Behördennetz durch einen dort eingerichteten zentralen Übergang integriert ist.

Es sind u.a. nachfolgende Sicherheitsmaßnahmen ergriffen:

- Trennung von anderen Benutzern auf o.a. Overlay-Netz auf OSI-Ebene 2 (Link Layer, Verbindungssicherungsschicht)
- kein Durchschleusen der Teilnehmeradressen
- Konfiguration als geschlossenes Multi-Protokollnetz

- Übergang zum Internet nur an einer zentralen Stelle
- Absicherung dieses Übergangs durch ein Firewall-System
- restriktive Freischaltung von Diensten und Ports
- verbindliche Sicherheitsgrundsätze für alle Teilnehmer
- Einrichtung eines zentralen Notfall- und Aktionsteams (CERT) mit weitreichenden Befugnissen
- Einrichtung weiterer CERT in den jeweiligen Subnetzen.

Der Zugang zum BYBN erfolgt in der Regel über Festverbindungen. Der Zugang über ISDN-Wählverbindungen zu einem Einwählknoten des Providers ist ebenfalls möglich. In diesem Fall wird zusätzlich eine Rufnummernidentifizierung durchgeführt und das Sicherheitsprotokoll CHAP (CHallenge Authentication Protocol) angewendet.

Angeschlossene Behörden können bei Bedarf und je nach Anschlußumfang ihre eigenen Netze oder besonders sensible Teile davon mit eigenen Firewall-Systemen, die vom zentralen CERT freigegeben oder vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert wurden, zusätzlich schützen. Dadurch sind im Bayerischen Behördennetz Kaskadierungen von Firewall-Systemen möglich. Grundsätzlich gilt, daß jede angeschlossene Behörde für ihr eigenes Netz selbst verantwortlich ist.

Der Zugangsschutz zu Diensten und Applikationen wird in erster Linie auf Anwendungsebene (meist durch Paßwortmechanismen) realisiert.

Da im BYBN das aus dem Internet bekannte TCP/IP als Standardprotokoll verwendet wird, sind zusätzliche Maßnahmen erforderlich, um auch innerhalb des Behördennetzes eine vertrauliche und nicht manipulierbare Datenübertragung zu gewährleisten. Dazu dienen die Bemühungen im Projekt BASILIKA. Der flächendeckende Einsatz dieser Lösungen steht aber noch aus, so daß die Sicherheit schutzwürdiger personenbezogener Daten bei der Übertragung über das Bayerische Behördennetz derzeit nicht in vollem Umfang gegeben ist. Hierauf habe ich die Staatskanzlei hingewiesen.

Sicherheitsarchitektur BASILIKA

Hauptrahmenbedingungen der für das Bayerische Behördennetz entwickelten Sicherheitsarchitektur sind

- die Verwendung von Standards und damit die Vermeidung proprietärer Lösungen,
- die Verwendung von zertifikatsbasierenden Protokollen (X.509),
- die Verwendung kryptographischer Funktionen, die frei sind von Key Recovery und Key Escrow-Mechanismen, d.h. europäische/deutsche Implementierungen, und
- die Verwendung von flexiblen und skalierbaren Lösungen.

Mit BASILIKA sollen abgedeckt werden:

- Verbindungsverschlüsselung durch Anwendung der Secure Socket Layer-Technologie (SSL V.3 in Verbindung mit TLS V.1) zur Herstellung sicherer Kanäle innerhalb des BYBN und sicherer Kanäle nach und von außen

Als Implementierungsmechanismen gelangen Sicherheitsproxies für Clients und Server, Single Sign On-Technologien und chipkartenfähige Produkte zum Einsatz. Diese Techniken werden in den Projekten Multifunktionale Chipkarte (MUCK) der Universität Würzburg und GEWAN (Gewerbeanmeldung) des Bayer. Landesamt für Statistik und Datenverarbeitung erprobt.

- Sichere E-Mail

Ziel ist es, eine Implementierungslösung zu finden, die in die im Behördennetz verwendeten Standardprodukte für elektronische Kommunikation integrierbar ist und auch sichere Mechanismen zur Verschlüsselung und digitalen Signatur auf Zertifikatsbasis bereitstellt.

- Sonstige gesicherte Datenübertragungsanforderungen durch Anwendung von generischen Sicherheitsdienste-API

Für besondere Anwendungen (z.B. Austausch von Patientendaten zwischen Ärzten) sollen entsprechende Anwendungsadapter (Schnittstelle zum HCP-Protokoll aus dem Bereich der Telemedizin) bereitgestellt werden.

Als Ergebnis von Praxistests wurde durch die Arbeitsgruppe "Sicherheit" im Sommer/Herbst 1998 eine Empfehlung zugunsten des Produktes TrustedMime zum Einsatz für sichere E-Mail

im Behördennetz ausgesprochen. Dadurch, daß TrustedMime im europäischen Raum entwickelt wurde, können die sich auch aus bestehenden Exportbeschränkungen ergebenden Nachteile für nicht-europäische Kryptoprodukte vermieden werden. Der Freistaat Bayern beabsichtigt, für TrustedMime eine Generallizenz zu erwerben. Zum Redaktionsschluß waren die Verhandlungen mit dem betreffenden Unternehmen leider noch nicht abgeschlossen.

Vor diesem Hintergrund befindet sich auch eine Zertifizierungsinfrastruktur für das Bayerische Behördennetz in Aufbau. Die Wurzelinstanz für die Verwaltung der öffentlichen Schlüssel für Verschlüsselung und Signatur wird beim Landesamt für Statistik und Datenverarbeitung eingerichtet (Trust Center, Certification Authority). Sie stellt auch den X.500-Verzeichnisdienst zur Verfügung. Bei den am BYBN teilnehmenden Behörden können bei Bedarf weitere Zertifizierungs- und Registrierungsinstanzen eingerichtet werden.

Ich begrüße die gewählten Ansätze in BASILIKA und die Entscheidung, nicht auf die Verfügbarkeit der technischen Komponenten und Sicherheitsinfrastruktur nach dem Signaturgesetz (siehe Abschnitt [19.1.4](#), "Einsatz kryptografischer Verfahren") zu warten. Die Bemühungen nach einem flächendeckenden Einsatz von Sicherheitskomponenten müssen rasch weiter vorangetrieben werden. Ein wichtiger Schritt ist mit der Entscheidung für TrustedMime und den Verhandlungen zum Erwerb einer Generallizenz bereits getan. Es kommt nun darauf an, die noch laufenden Verhandlungen bald zu einem erfolgreichen Abschluß zu bringen und dieses Produkt auch rasch zur Absicherung von E-Mail flächendeckend einzusetzen.

Erst wenn alle derzeit bekannten Schwachstellen beseitigt sind, kann das Bayerische Behördennetz auch den erwarteten Nutzen für die Verwaltung bringen. Auf die Sicherheitslücken habe ich - wie bemerkt - mehrfach hingewiesen. Ich werde die Entwicklungen weiter verfolgen. Eine Nutzung dieses offenen Netzes für die Übermittlung von personenbezogenen Informationen, ohne Einsatz entsprechender Sicherheitsmaßnahmen, werde ich beanstanden.

Zentrale Übergänge zu anderen Auskunftssystemen

Ein weiteres wesentliches Ziel des Bayerischen Behördennetzes ist die Reduzierung der bisher anfallenden, z.T. recht hohen Kommunikationskosten mit anderen zentralen Systemen. Aus diesem Grund hat das LfStaD in enger Abstimmung mit dem Bundesverwaltungsamt im Behördennetz einen zentralen Zugang zum Ausländerzentralregister (AZR) bereitgestellt.

Dabei wurden eine ganze Reihe weiterer Sicherheitsmaßnahmen, die über die sonstigen, im Behördennetz vorhandenen Maßnahmen hinausgehen, ergriffen. Es konnten die im AZR üblichen

Zugangs- und Zugriffsschutzmechanismen unverändert beibehalten und bzgl. der Berechtigungserteilung und ihrer Revisionsfähigkeit für bayerische Zugangsberechtigte erhöht werden. Für die Übertragung der Daten über das Behördennetz von und zum jeweiligen Arbeitsplatz ist, wie oben dargestellt, die Sicherstellung der Vertraulichkeit und Integrität derzeit noch nicht gegeben. Mit flächendeckender Verfügbarkeit der entsprechenden Komponenten aus BASILIKA sollen diese eingesetzt und diese Schwachstelle geschlossen werden. Ich werde die Bemühungen weiter aufmerksam begleiten.

Eine vergleichbare Lösung untersucht das LfStaD auch für die Anbindung des Behördennetzes an das Kraftfahrtbundesamt (KBA) und weitere zentrale Systeme.

19.3.2 Überlegungen zum Outsourcing von DV-Leistungen

Outsourcing ist ein Begriff, der immer häufiger pauschal und insbesondere im Zusammenhang mit Einsparungspotential bei unterschiedlichen Ressourcen (auch Personal) in die Diskussion eingebracht wird. Dabei ist jedoch zu präzisieren, was mit Outsourcing im konkreten Einzelfall gemeint ist, d.h. welche Leistungen nicht selbst erledigt, sondern an Dritte (meist Privatfirmen) abgegeben werden.

Grundsätzlich kommen beispielsweise folgende DV-Aufgaben für eine Vergabe außer Haus in Betracht:

- Konzeption von DV-Systemen und Netzwerken
- Entwicklung, Wartung und Pflege von Software
- Wartung von Hardware
- Administration einzelner Rechnersysteme (z.B. Firewall-Rechner)
- Administration von Netzwerken
- Bereitstellung und Betrieb von Rechnersystemen
- Bereitstellung und Betrieb ganzer Rechenzentren
- Abwicklung von sonstigen DV-Arbeiten (z.B. Datenerfassung, Datenpflege)
- Bereitstellung von Backup-Systemen
- Vollständige Abwicklung ganzer DV-Aufgaben.

Eine pauschale Bewertung und Aussage, welche Datenschutz- und Datensicherungsmaßnahmen bei welchem Umfang von Outsourcing notwendig und angemessen sind, läßt sich selten treffen.

Es ist stets eine Einzelfallprüfung erforderlich. Hinzu kommt, daß natürlich die Art der gespeicherten, be- und verarbeiteten Daten hinsichtlich ihrer besonderen Schutzbedürftigkeit berücksichtigt werden muß (vgl. Outsourcing im Krankenhausbereich, [Nr. 3.3.5](#)), so daß schon aus diesen Gründen das Outsourcing vielfach ausscheiden wird. Im übrigen kann gerade in solchen Fällen sehr schnell der Zustand erreicht werden, daß die Erreichung der mit dem Outsourcing angestrebten Ziele (Einsparung von Ressourcen) aufgrund der zu ergreifenden Datenschutz- und Datensicherungsmaßnahmen in Frage gestellt oder gar verfehlt wird. Auch eine Wirtschaftlichkeitsbetrachtung der Outsourcingmaßnahme unter Berücksichtigung des Aufwandes für die erforderlichen Sicherheitsmaßnahmen ist hier dringend geboten.

Nach einer Untersuchung der Gartner Group wird das weltweite Outsourcing-Geschäft in den Bereichen "Netzwerk" und "PC/LAN" von 5,6 Milliarden Dollars im Jahre 1995 auf etwa 17 Milliarden Dollars im Jahre 2000 steigen, sich also etwa verdreifachen. Im Vergleich dazu wird sich das klassische Outsourcing-Segment "Rechenzentrum" nur von 10,2 Milliarden auf 17,9 Milliarden Dollars erhöhen.

Als Hauptgründe dafür werden angesehen: Die zunehmende Vernetzung und die ständig steigende Leistungsfähigkeit der DV-Systeme erfordern auch einen immer höheren Betreuungsaufwand, den sich kleinere Institutionen, mittlere Unternehmen oder kostenbewußte DV-Anwender nicht mehr leisten können oder wollen. Deshalb bieten externe Dienstleister, die sich auf eine bestimmte Dienstleistung spezialisiert haben und über ein kompetentes Expertenteam verfügen, vermehrt DV-Services der unterschiedlichsten Art an, um den Anwender bei schwierigen Spezialaufgaben zu entlasten.

Bei an Private vergebenen Datenverarbeitungsaufgaben handelte es sich früher meist um Datenerfassungs- und Versandarbeiten. Die Datenerfassung spielt heute eine geringe Bedeutung, weil sie meist im Rahmen der Sachbearbeitung erledigt wird, hingegen ist das Auslagern von Versandarbeiten (ePost) im Kommen. Auch das Vorhalten von Backup-Kapazitäten für den Katastrophenfall ist heute noch ein klassisches Outsourcing-Feld. Viele Institutionen haben ihre DV-Aktivitäten in ein einziges Rechenzentrum verlagert. Diese Entwicklung wurde durch die ständig leistungsfähiger werdenden Rechner begünstigt, die immer mehr Endanwender versorgen können. Im Katastrophenfall weicht man dann meist auf einen Backup-Rechner eines Dienstleisters oder des Herstellers aus.

Es gibt aber auch Beispiele, bei denen sich das Vorhalten eigener Ressourcen überhaupt nicht

rechnet, wie die Herstellung der Krankenversichertenkarte. Für diesen Prozeß gibt es Spezialfirmen, die die Chipkarten für die Krankenkassen herstellen und gleich an die Versicherten versenden. Auch die DATEV e.V. in Nürnberg betreut viele Steuerberater in Deutschland DV-technisch.

In all diesen Fällen behält der Auftraggeber jedoch stets die Verfügungsgewalt über seine Daten. Auf die Fälle, bei denen eine Funktionsübertragung stattfindet, soll an dieser Stelle nicht näher eingegangen werden.

19.3.3 Rechenzentrumssicherheit

Während früher in den einzelnen Geschäftsbereichen häufig mehrere Rechenzentren an unterschiedlichen Standorten betrieben wurden, die bei Ausfall eines Rechners gegenseitig die Funktion als Backup-Rechner übernehmen konnten, zeichnet sich heute eine Entwicklung zur Konzentration der Rechnerkapazitäten in einem einzigen Rechenzentrum ab. Diese Lösung ist zwar sehr wirtschaftlich, enthält aber häufig gravierende Sicherheitsmängel, wenn bei der Planung an der Investition für geeignete Sicherheitsmaßnahmen gespart wurde. Der Ausfall eines solchen zentralen Rechners kann die betroffene Stelle unter Umständen tagelang lahm legen. Um das Ausfallrisiko möglichst klein zu halten, muß man sich gut überlegen, wo solche Rechenzentren eingerichtet werden. Am besten ist es, für solche Rechenzentren eigene Sicherheitstrakte in einem separaten Gebäude vorzusehen, damit Brand- und Sabotagerisiken minimiert werden. Fremde Personen und Behördenbesucher haben dann in solchen Gebäuden nichts verloren. Um die Verfügbarkeit der automatisierten Datenverarbeitung zu erhöhen, sind schließlich geeignete Notfallkonzepte zu entwickeln und regelmäßig zu proben. Meist ist es weniger die Hardware, die in der Regel kurzfristig vom Hersteller zur Verfügung gestellt werden kann, als die in Mitleidenschaft gezogene DV-Infrastruktur (Verkabelung etc.) oder die fehlenden Räumlichkeiten, die eine Wiederaufnahme des Rechenbetriebs verzögern. Ein Notfallkonzept ist demnach unzureichend, wenn lediglich mit dem Hardwarehersteller Vereinbarungen über eine Ersatzstellung von DV-Geräten getroffen wurden.

19.3.4 Sicherheitsmaßnahmen bei automatisierten Krankenhausverwaltungssystemen

Die Automatisierung im Krankenhaus schreitet stetig voran. Zwar ist man von einer elektronischen Krankenakte noch weit entfernt, in Teilbereichen ist sie allerdings schon Realität geworden, wenngleich wegen der Vollständigkeit und Beweissicherheit auf die Papierdokumentation nicht verzichtet werden kann. Vor Jahren beschränkte man sich bei der Datenverarbeitung im Krankenhaus auf die Patientenabrechnung, die damals noch ohne medizinische Daten auskam. Die auf dem Markt befindlichen Patientenverwaltungssysteme sehen heute stets die Speicherung medizinischer Patientendaten vor. Diese Daten unterliegen der ärztlichen Schweigepflicht, so daß auf sie nur zugreifen kann, wer mit der Behandlung des Patienten betraut ist. Das bedingt wiederum, daß die zum Einsatz kommenden DV-Systeme das im Krankenhaus übliche Zugriffsschutzkonzept abbilden können.

Die Vielfalt der auf dem Markt angebotenen Patientenverwaltungssysteme ist derzeit noch recht groß, so daß uns die unterschiedlichsten Systeme begegnen, deren Sicherheitsfunktionen häufig unterschiedlicher Qualität sind. Je nach Leistungsfähigkeit und Komplexität des Systems wird meist ein hohes Maß an DV-Wissen an Anwender, Betreiber und Prüfinstanz gestellt. Die Prüfungen haben deshalb auch gezeigt, daß der Betreiber eine Reihe qualifizierter Mitarbeiter bereitstellen muß, wenn er einen ordnungsgemäßen Betrieb des Systems sicherstellen will. Zwar kann der Betreiber auch die Hilfe des Herstellers in Anspruch nehmen, das kostet aber in der Regel viel Geld und trägt obendrein noch dazu bei, daß die Anwender oft im Unklaren über Stärken und Schwächen des jeweiligen Systems gelassen werden. Ein sicherer Betrieb setzt gezielte Kenntnisse des eingesetzten Systems voraus, auch die Prüfung der Einhaltung der gebotenen Sicherheitsmaßnahmen ist nur mit entsprechenden Systemkenntnissen möglich. Daraus folgt, daß der Betreiber eine Reihe qualifizierter, gut geschulter Mitarbeiter für die Einhaltung eines ordnungsgemäßen Betriebs abstellen muß. Tut er das nicht, können Sicherheitsdefizite entstehen, die letztlich auch dazu führen können, daß Unbefugte unbemerkt Zugriff auf Patientendaten erhalten. Mächtige DV-Systeme können einerseits bei mangelhafter Generierung nicht vorgesehene Aktionen zulassen, die Qualität der Verarbeitung nachhaltig verändern, andererseits aber auch nicht gewünschte Veränderungen der Organisationsform initiieren. Solche Begleiterscheinungen gilt es möglichst frühzeitig zu untersuchen und datenschutzrechtlich zu bewerten.

Entscheidend für den ordnungsgemäßen Einsatz eines DV-Systems ist seine Benutzerfreundlichkeit. Diese Erkenntnis ist zwar nicht neu, verdient aber, immer wieder erwähnt zu werden. Eine gründliche Schulung aller Benutzer ist für einen reibungslosen Einsatz unerlässlich. Die Sicherheitsmaßnahmen müssen sich außerdem an der Organisation der einsetzenden Stelle orientieren, damit sie von den Benutzern akzeptiert werden. Schwierig zu handhabende Maßnahmen verfehlen bekanntlich ihren Schutzzweck, weil sie sonst nicht oder nur mangelhaft genutzt werden.

Wegen der besonderen Sensibilität medizinischer Daten müssen die Sicherheitsmaßnahmen auch von besonders hoher Qualität sein. Patientenverwaltungssysteme müssen deshalb im einzelnen nachfolgende Forderungen erfüllen:

Jeder Bedienstete darf nur auf die Daten zugreifen können, die er für seine Aufgabenerfüllung bzw. für die Behandlung der ihm anvertrauten Patienten benötigt. In der Praxis wird das durch die Einrichtung **benutzerbezogener Zugriffsberechtigungen** gelöst (vgl. hierzu in rechtlicher Hinsicht unter [Nr. 3.3.2](#) dieses Tätigkeitsberichts). Die Systeme müssen deshalb über einen sog. Profilergenerator verfügen, der die Einrichtung bedarfsgerechter Zugriffsberechtigungen unterstützt. Meist lassen sich bestimmte Benutzerprofile zu Gruppenprofilen zusammenfassen. In einem größeren Krankenhaus wird man trotzdem auf eine ganze Anzahl unterschiedlicher Gruppenprofile kommen. Die Zugriffsberechtigungen müssen auch **revisionsfähig** sein, das heißt, es muß eine Dokumentation vorhanden sein, aus der hervorgeht, wer über welchen Zeitraum über welche Zugriffsberechtigungen verfügte. Nur so wird sichergestellt, daß nachträglich eine Überprüfung der Zugriffsberechtigungen möglich ist. Das System muß auch Überweisungen an andere Abteilungen innerhalb eines Krankenhauses abbilden können.

Der Zugriff muß mindestens über **Benutzerkennung und Paßwort** gesteuert sein. Als Identifikationsmedium ist jedoch die **Chipkarte** anzustreben, die zusätzlich über ein Paßwort aktiviert wird. Diese Chipkarte sollte außerdem für die Dauer des Dialogs im Lesegerät der Datenstation stecken bleiben. Das Entfernen der Chipkarte muß für eine Dunkelschaltung des Bildschirms und eine Unterbrechung des Dialogs, die nur mit der Chipkarte (und Eingabe des Paßworts) wieder aufgehoben werden kann, sorgen. Diese Funktionen sind gerade im Stationsbereich, wo die Arbeit am Bildschirm häufig unterbrochen werden muß, von sehr großem Nutzen.

Werden die Daten eines Patienten nicht mehr benötigt, beispielsweise wenn die Behandlung abgeschlossen ist, sind sie zu **sperren**. Eine Aufhebung der Sperre kann nur derjenige veranlassen, der dazu aufgrund seiner Aufgabenerfüllung (u.a. Wiederaufnahme des Patienten im Kranken-

haus) dazu berechtigt ist. Denkbar wäre, daß auf Altpatienten nur unter bestimmten Kennungen und von bestimmten Rechnern bei gleichzeitiger Protokollierung der lesenden Zugriffe zugegriffen werden kann.

Gespeicherte medizinische Patientendaten (elektronische Patientenakte) sind so abzusichern, daß sie nicht mehr geändert oder gelöscht werden können. Die **Manipulationssicherheit** ist eine der wichtigsten Sicherheitsmaßnahmen. Schließlich muß erkennbar sein, wer für die Korrektheit der gespeicherten Patientendaten verantwortlich ist ("Signierung") und wann die Daten eingespeichert wurden.

Im Rahmen der **Beweissicherung** muß das System bestimmte Protokollaufzeichnungen unterstützen. Zum einen müssen alle vom System als Sicherheitsverletzungen erkannte Aktionen revisionsfähig und benutzerfreundlich protokolliert werden. Ebenso sind alle Aktionen der Wartung am Anwendungssystem zu protokollieren, daß diese Einträge von sachverständigen Dritten ausgewertet werden können.

Lesende Zugriffe sind immer dann zu **protokollieren**, wenn der Zugriff über Kennungen erfolgt, die keinen restriktiven Zugriffsbeschränkungen unterworfen sind, beispielsweise für Notärzte, die Zugriff auf alle Patienten haben müssen (Analogie zum automatisierten Abrufverfahren). Für solche Zugriffe sind in einer speziellen Protokolldatei Zeitstempel, Benutzerkennung, Patientenummer und eventuell die Ursache für den Zugriff festzuhalten.

Bei meinen Prüfungen in Krankenhäusern konnte ich feststellen, daß manche Sicherheitsmaßnahmen noch realisiert werden müssen.

19.3.5 Krankenhaus am Internet

Im Berichtszeitraum wurde immer wieder die Frage an mich heran getragen, unter welchen Umständen Krankenhäuser sich der Vorteile des Internets als Informationsquelle und als Transportnetz zu Nutzen machen können.

Beim Anschluß eines Krankenhauses ans Internet ist auf die Einhaltung folgender Sicherheitsmaßnahmen zu achten:

Wird das interne Netz durch einen geeigneten Firewall-Rechner vom Internet abgeschottet, kann von jedem Client aus auf das Internet zugegriffen werden. Fehlt ein Firewall-Rechner, muß das interne Netz von solchen Rechnern getrennt werden, die Verbindung zum Internet aufnehmen

können. Da eine physikalische Trennung meist Medienbrüche verursacht und schwer zu kontrollieren ist, ob die Trennung in jedem Falle eingehalten wird, sollte der ersten Alternative der Vorzug gegeben werden. Außerdem ist zu beachten, daß das Internet heute umfangreiche Informationsmöglichkeiten (Health Online, Gesundheitsdienst) eröffnet, von denen Ärzte zunehmend Gebrauch machen werden.

Beim Versand von Arztbriefen über das Internet ist zu berücksichtigen, daß das Internet ein offenes Netz ist, das keinerlei Vertraulichkeit bietet. Aus diesem Grunde sind alle über das Internet zu versendenden Dokumente vertraulichen Inhalts vorher zu verschlüsseln. Als hinreichend sichere Algorithmen gelten beispielsweise Triple-DES, RSA und IDEA. Geeignete Softwareprodukte stehen im Internet sowie auf dem Markt zur Verfügung. Es wird empfohlen, eine Schlüssellänge von wenigstens 512 Bit zu verwenden.

19.3.6 Telearbeit

Bereits im 17. TB wurden unter der Textziffer [18.3.3](#) einige Sicherheitsanforderungen an Telearbeitsplätze vorgeschlagen. Zum damaligen Zeitpunkt waren jedoch nur ganz vereinzelt Arbeitsplätze anzutreffen. In der Zwischenzeit hat die gesamte maschinelle Datenverarbeitung durch die Möglichkeiten des Internet oder Intranet eine rasante Fortentwicklung erfahren, wovon nicht zuletzt auch die Telearbeitsplätze profitieren können. Allerdings haben sich damit auch die Risiken erhöht, denen man wiederum durch höherwertige Sicherheitsmaßnahmen begegnen muß. Über die allgemeinen Vor- und Nachteile von Telearbeitsplätzen braucht man an dieser Stelle keine Worte verlieren, dazu sind in der einschlägigen Literatur zahlreiche interessante Beiträge zu finden. Unbeschadet der technischen und organisatorischen Maßnahmen bleibt aber festzuhalten, daß bei der Telearbeit der Personalrat zu beteiligen ist und Art und Umfang der Telearbeit häufig mit der Personalvertretung in einer Personalvereinbarung geregelt wird..

Im Prinzip sind auch für Telearbeitsplätze die Vorgaben, wie sie für die Auftragsdatenverarbeitung gelten, anzuwenden. Aufgaben, die nicht außer Haus (an Dritte) gegeben werden dürfen, eignen sich auch nicht, in Telearbeit erledigt zu werden.

Da die datenverarbeitende Stelle die unmittelbare Verfügungsgewalt über die Daten verliert, sind vertragliche Vereinbarungen über die Telearbeit zwischen dem Arbeitgeber bzw. Dienstherrn auf der einen Seite und den Beschäftigten auf der anderen Seite notwendig. In diesen schriftlichen

Vereinbarungen sind Art und Umfang der Aufgaben und die Rahmenbedingungen, unter denen die Aufgaben abzulaufen haben, zu definieren. Sie müssen außerdem detaillierte Aussagen über die Pflichten der in Telearbeit stehenden Mitarbeiter enthalten, was letztlich auch in Form eines Vertrages oder einer Dienstanweisung geschehen kann. Der in Telearbeit stehende Mitarbeiter muß schließlich über die Risiken aufgeklärt werden.

Bei der Telearbeit werden die erforderlichen IT-Geräte, die für die Verarbeitung notwendige Software und die Telekommunikationsverbindungen vom Arbeitgeber gestellt. Nur in begründeten Ausnahmefällen sollte die Verwendung privater IT-Komponenten gestattet sein. Die Schulung und Einweisung in die DV-Systeme wird ebenso vom Arbeitgeber vorgenommen, wie die Systemadministration. Eine zentrale Systemadministration garantiert einen reibungslosen Ablauf der Arbeiten und vermindert Störungen.

Entsprechend der Schutzbedürftigkeit der verarbeiteten Daten sind angemessene Sicherheitsmaßnahmen zu ergreifen, die eine unbefugte Systemnutzung und einen unberechtigten Zugriff auf die gespeicherten Daten ausschließen. Gefährdungen können am Telearbeitsplatz (Diebstahl von IT-Komponenten, unberechtigte Kenntnisnahme von Informationen, Verlust der Verfügbarkeit der Daten durch technische Störungen), auf den Telekommunikationsverbindungen (Verlust der Integrität und Vertraulichkeit der Daten) sowie bei der Anbindung der IT-Komponenten selbst (Anschluß an offene Netze) entstehen.

Folgende Maßnahmen können die Datensicherheit entscheidend verbessern:

- Identifikation und Authentisierung als Maßnahmen der Zugriffskontrolle (mittels Paßwort u.U. mit Chipkarte gekoppelt) und Verschlüsselung der gespeicherten Daten als Maßnahme zur Sicherung der Vertraulichkeit bei Diebstahl des Computers
- Begrenzte Speicherhaltung der Nutzdaten, sofern sie für eine weitere Bearbeitung nicht mehr benötigt werden. Aus Gründen der Datensicherheit empfiehlt es sich, wenn man für Recherchezwecke auf einen zentralen Datenbestand beim Arbeitgeber zugreift und somit eine dezentrale Speicherung des Datenbestands vermeidet.
- Einsatz eines Virenschanner zum Schutze vor einem Virenbefall (von Diskette oder über Leitung)
- Die Datenkommunikation über Leitungen mit dem zentralen Rechner ist aus Gründen der Vertraulichkeit nur in verschlüsselter Form durchzuführen; beim Datenträgeraustausch auf dem Postweg (sofern vorgesehen) sollte ebenfalls verschlüsselt werden.

- Alle dienstlichen Unterlagen sind verschlossen aufzubewahren, damit Unbefugte keine Kenntnis von den Inhalten dieser Unterlagen nehmen können.
- Um den Benutzer zu entlasten und Bedienungsfehlern vorzubeugen, empfiehlt es sich, die Datensicherung von der Zentrale aus anzustoßen und die Sicherungsbestände auch zentral zu verwalten. Dem Benutzer bleiben somit alle notwendigen Backup-Maßnahmen erspart, und im Notfall oder nach einer schwerwiegenden Systemstörung ist ein schneller Wiederanlauf damit gewährleistet.
- Der Arbeitnehmer stimmt in der Betriebsvereinbarung dem Kontrollrecht des Arbeitgebers und des Datenschutzbeauftragten zu. In einem Merkblatt, das dem Telearbeiter ausgehändigt wird, sollen alle Regelungen, insbesondere die Notfallmaßnahmen (Aktionen und Ansprechpartner) zusammengefaßt werden.
- Die vom Dienstherrn zur Verfügung gestellte technische Infrastruktur ist nur für dienstliche Zwecke und nur vom Arbeitnehmer selbst zu verwenden.
- Zur Sicherung der Kommunikationsanschlüsse bieten sich am zentralen Rechner der Einsatz spezieller Kommunikationsrechner, einer Call-Back-Funktion und sicherer Identifikations- und Authentisierungsmechanismen an. Am dezentralen System ist durch spezielle Maßnahmen Sorge zu tragen, daß ausschließlich erlaubte Kommunikationsverbindungen hergestellt werden können. Ist ein Zugang zum Internet nicht erforderlich, ist dieser zu sperren, um teure Abschottungsmaßnahmen (Firewall-Systeme) zu sparen.

19.3.7 Protokollierung von lesenden Zugriffen

Betriebssysteme, systemnahe Software und Anwendungsprogramme zeichnen in der Regel eine Reihe von Benutzungsdaten auf. Diese Benutzungsdaten, auch Ablaufdaten genannt, werden in sog. Log-Dateien (Protokolldateien) abgespeichert. Sie dienen in erster Linie der Beweissicherung eines ordnungsgemäßen Ablaufs von DV-Aktionen. Sie sind jedoch auch für eine **nachträgliche** Kontrolle von Benutzeraktivitäten, insbesondere für die Datenschutzkontrolle geeignet.

Die Protokolldaten sind personenbezogen, da sie Aufschluß über die Aktivitäten eines Benutzers geben. Sie unterliegen nach dem Datenschutzrecht einer strikten Zweckbindung ([Art. 17 Abs. 4 BayDSG](#)) und dürfen nur zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbei-

tung oder zur Aufdeckung von mißbräuchlichen Zugriffen oder Zugriffsversuchen, keinesfalls jedoch für Zwecke der Verhaltens- oder Leistungskontrolle der Mitarbeiter verwendet oder ausgewertet werden. Es empfiehlt sich deshalb, die Personalvertretung bei der Festlegung der zulässigen Auswertungen bzw. bei der Kontrolle der Protokolldateien sowie der Art ihrer sonstigen Nutzung rechtzeitig einzubinden.

In der Praxis wird auf die Protokollierung von lesenden Satzzugriffen meist verzichtet, da den Benutzern ein aufgabenbezogenes Zugriffsberechtigungsprofil zugeordnet wurde, so daß Lese- und Schreibzugriffe nur im Rahmen dieser Zugriffsberechtigung auftreten können. Schreibende Zugriffe, wie Einfügen, Ändern, Löschen, werden in vielen Anwendungen ohnehin veranlasserbezogen festgehalten, so daß für einen festgelegten Zeitraum dokumentiert bleibt, wer aus welchem Grund was verändert hat. Auch Datenbanksysteme protokollieren alle schreibenden Zugriffe.

Die Aufzeichnung von solchen Lesezugriffen würde zu dem in vielen Fällen eine Unmenge von Protokoll Daten erzeugen, die für die Kontrolle der Zugriffsberechtigung eigentlich irrelevant sind, weil diese bereits vorher maschinell erfolgt ist.

Es gibt jedoch Ausnahmen, bei denen auch die Protokollierung von satzbezogenen Lesezugriffen für eine effektive Beweissicherung Sinn macht, nämlich bei automatisierten Abrufverfahren (Übermittlung i. S. des Datenschutzrechts).

Beispiele für automatisierte Abrufe aus dem öffentlichen Bereich sind Abrufe beim maschinellen Grundbuch (SOLUM STAR), beim Kfz-Halter-Register des Kraftfahrt-Bundesamts oder beim Ausländerzentralregister.

Bei manchen Verfahren wird wegen der Menge der Abfragen nur stichprobenweise protokolliert. Eine Protokollierung eines satzbezogenen Zugriffs kann auch bei der Patientenstammdatei eines großen Klinikums geboten sein, wenn Ärzte anderer Abteilungen zur Behandlung bestimmter Patienten beratend hinzugezogen werden, so daß ihnen ein Zugriff auf diese Patienten eröffnet werden muß.

Für einen solchen Fall bietet sich für den Benutzer die Einrichtung zweier Zugriffskennungen an:

- eine Kennung für ihn als behandelnder Stationsarzt für den Zugriff auf alle Patienten seiner Station (keine Protokollierung),
- eine andere Kennung für ihn als diensthabenden Notarzt oder hinzugezogenen Konsiliaris (sog. Generalschlüssel) mit dem umfassenden Zugriff auf alle Patienten (Protokollierung des satzbezogenen Zugriffs).

Im Prinzip wäre auch eine satzweise Freischaltung des Zugriffs möglich. Eine solche Vorgehensweise wäre jedoch vom Handling her viel zu aufwendig. Deshalb wird dieser Kennung der gesamte Datenbestand zur Verfügung gestellt und jeder Zugriff für spätere Kontrollzwecke protokolliert.

19.3.8 Hoax-Viren und Hostile Applets

Die Unkenntnis der Funktionsweise von Viren und die Tatsache, daß immer mehr Computerviren und Trojanische Pferde auftauchen, führt seit Jahren dazu, daß den über das Internet mittels E-Mail verbreiteten Warnungen, Hinweisen und Informationen zu Computerviren zunehmend mehr Beachtung geschenkt wird. Bei der Menge dieser Meldungen ist es kaum noch möglich, diese auf Echtheit zu überprüfen. Diese Tatsache ist der ideale Nährboden für eine neue Virenart, die sich rapide ausbreitet, den sogenannten Hoaxes. Ein Hoax (Bluff oder schlechter Scherz) ist eine **Falschmeldung**, die vor einem nicht vorhandenen Virus warnt und damit zu einer großen Verunsicherung der Anwender und Verantwortlichen und zu bedeutenden finanziellen Schäden führen kann. Diese Falschmeldungen werden zum Teil ohne Berücksichtigung der Konsequenzen bewußt erzeugt und versandt. Zumeist werden die Empfänger aufgefordert, diese Mitteilung an möglichst viele Anwender weiterzuleiten. Damit wird der Empfänger unbewußt zum "Virenüberträger", da er wiederum beim neuen Empfänger eine Verunsicherung - "den Schadensteil" - auslöst.

Bekannteste Beispiele sind "Good Times" (mit den Varianten "Deeyenda", "Join the crew" und "Penpal Greetings") sowie "Irina".

Auch wenn diese Hoaxes keine Systeme unmittelbar befallen, so muß doch immer mehr Aufwand betrieben werden, um Falschmeldungen von echten Viren zu unterscheiden. Zudem können Hoaxes dazu eingesetzt werden, Empfänger zu manipulieren. Hoaxes müssen zu der Gattung

der Viren gezählt werden, da sie

- sich ausbreiten (sie werden per E-Mail repliziert),
- eine Wirkung haben (zumindest einen Zeitaufwand, um echte von falschen Warnungen zu unterscheiden) sowie
- einen Wirt zu ihrer Vermehrung benutzen (der Adressat einer Warnung folgt der Aufforderung und verteilt die Warnung an weitere Anwender).

Folgende Punkte sollten deshalb beim Empfang von E-Mails beachtet werden:

- Durch das alleinige **Lesen** einer E-Mail wird der Computer durch Hoaxes noch nicht infiziert. Dies kann sich allerdings durch den Einsatz des Betriebssystems Windows 98 und der Komponenten Outlook 98 bzw. Outlook Express ändern. Diese Programme können E-Mails im HTML-Format versenden und empfangen. Im HTML-Code kann jedoch eine Programmerroutine (in Visual Basic) versteckt sein, die den Zugriff auf das Dateisystem des Empfängerrechners ermöglicht. Damit könnte das in der Mail versteckte Programm Dateien löschen, Trojanische Pferde einschleusen oder sonstige Viren installieren. Um sich als Outlook-Benutzer gegen einen Virenbefall zu schützen, muß die **Sicherheitsstufe im Internet Explorer** über das Menü "Ansicht/(Internet)optionen/Sicherheit" auf "Hoch (am sichersten)" eingestellt sein. Dies verhindert die Ausführung der automatischen Programmroutine in den E-Mails. Diese Einstellung wirkt sich auch auf Outlook aus, weil Outlook den Internet Explorer zum Anzeigen der HTML-Mails verwendet. Allerdings kann der Internet Explorer bei dieser Einstellung generell keine Visual-Basic-Scripts mehr verarbeiten, was zu Fehlermeldungen beim Internet-Surfen führt.
- Ein Anhang (Attachment) einer E-Mail kann ein ausführbares Programm oder einen Makrocode (z. B. zur Ausführung in Word-Dokumenten) enthalten. Beide können bei einem Öffnen des Attachments mit Doppelklick den Rechner mit einem Virus verseuchen.

Immer mehr in den Mittelpunkt rücken auch sogenannte **Hostile Applets** - also feindliche Anwendungen - aus dem Internet. Diese Art von Viren wird in der immer mächtiger werdenden plattformübergreifenden Programmiersprache **Java** geschrieben oder als **ActiveX**-Control für den Microsoft Internet Explorer verkleidet. Zu den Hostile Applets zählen auch Viren in Form von Trojanischen Pferden, die zum Beispiel Daten innerhalb einer Behörde sammeln können und diese an Dritte versenden. Ein aktuelle Beispiel hierfür sind die "T-Online-Powertoys", eine Software, die durchaus nützliche Hilfsprogramme zum T-Online-Dekoder enthält. Bei der On-

line-Registrierung dieser Software werden aber auch die Benutzerkennung und das auf der Festplatte gespeicherte Paßwort zum T-Online-Aufruf ausgelesen und an dem Empfänger der Registrierung weitergeleitet.

Dies zeigt einmal mehr, wie wichtig heutzutage Antivirenprogramme sind. Mit diesen Programmen müssen auch die Internetübergänge, E-Mails, Server und die einzelnen Arbeitsstationen überwacht werden.

19.3.9 Systemunterstützung im Kommunalbereich durch die AKDB

Wie bereits oben erwähnt, haben kleinere Dienststellen einen größeren Systemberatungsbedarf, weil sie sich aufgrund ihrer Personaldecke kaum EDV-Experten leisten können. Das trifft vor allem für den Großteil der bayerischen Gemeinden zu. Während die Anwenderbetreuung meist noch von einem Bediensteten der Dienststelle erledigt wird, benötigt man bei Systemfragen externen Sachverstand, der meist von dem Ersteller des DV-Systems kommt. In einigen Gemeinden hat man mit dem Hard- sowie Systemsoftwarelieferant und dem Lieferanten der Anwendungssoftware sogar zwei Ansprechpartner. Die Kommunikation erfolgt in der Regel online über ISDN-Leitung.

Seit Mitte 1998 hat die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) ein System im Einsatz, das alle Aktionen einer Tele-Systemunterstützung protokolliert. In einer Datei werden wie bei einem Video alle Bildschirminhalte und Aktionen aufgezeichnet, wobei diese Datei durch ein Checksummenverfahren gegen nachträgliche Manipulationen abgesichert ist. Es ist also möglich, zu einem späteren Zeitpunkt, etwa für Revisions- und Prüfzwecke den gesamten Dialog zeitgenau noch einmal ablaufen zu lassen. Dieses Verfahren wird für alle Fernwartungsaktivitäten und Systemunterstützungen angewandt; die Möglichkeit der Datenübertragung von und zur Dienststelle ist ebenfalls gegeben. Vor Ort kann der Systemverantwortliche den gesamten Dialog mitverfolgen und gegebenenfalls jederzeit abbrechen. Zusätzliche Sicherheitsmaßnahmen sind: Verbindungsaufbau nach dem Call-Back-Verfahren und Verschlüsselung des gesamten Dialogs (auf Routerbasis).

19.3.10 Mechanische Sicherungen

Trotz der zunehmenden Automatisierung und Vernetzung ist ein papierloses Büro nach wie vor Zukunftsmusik. Die Verwaltung ist bei der Aufgabenerledigung immer noch auf konventionell geführte Akten und Karteien angewiesen. Diese Bestände enthalten auch vielfach recht sensible personenbezogene Daten. Zum Schutze dieser Daten empfehle ich stets geeignete mechanische Sicherungsmaßnahmen, damit diese Daten nicht zu leicht in unrechte Hände gelangen können. Einige Sachversicherer berichteten nun, daß die Anzahl der Einbrüche auch in öffentliche Einrichtungen in den letzten Jahren stark zugenommen habe. Ziel dieser Einbrüche seien Wertgegenstände, wie Bargeld oder technisches Equipment. Da Zimmer- und Schranktüren nach Dienstschluß verschlossen würden, seien die Schäden, die durch den Aufbruch dieser Türen entstanden sind, oft größer, als die eigentlichen Diebstahlsschäden. Die Sachversicherer empfehlen deshalb, Zimmer- und Schranktüren außerhalb der Dienstzeit nicht abzuschließen und stärkeres Gewicht auf die Installation einer geeigneten Einbruchmeldeanlage zu legen, die manche Einbrüche von vornherein verhindern kann.

Diese Betrachtungsweise kann aus der Sicht des Datenschutzbeauftragten nicht geteilt werden. Eine Einbruchmeldeanlage wird in der Regel erst dann aktiviert, wenn der letzte Bedienstete das Haus verlassen hat. Maßnahmen gegen unberechtigte Kenntnisnahme von personenbezogenen Daten richten sich jedoch nicht allein gegen Eindringlinge von außen, sondern in erster Linie gegen Insider, Besucher und gegen den Reinigungsdienst, der zu meinen Bedauern häufig von Fremdfirmen erledigt wird. Kriminelle Eindringlinge haben es meines Erachtens kaum auf Aktenschränke abgesehen, wenn diese als solche erkennbar sind, so daß Aktenschränke durchaus verschlossen zu halten sind.

Sorgen bereiten aber die zahlreichen DV-Geräte, die in den ungesicherten Büroräumen der Bediensteten stehen. Werden auf diesen Geräten personenbezogene Daten unverschlüsselt gespeichert, wovon man in der Regel eigentlich ausgehen kann, so gelangen diese bei Diebstahl des Computers in fremde Hände. Ein wirksamer Schutz solcher Daten läßt sich eigentlich nur dadurch erreichen, daß alle Datenbestände und sensiblen Schriftstücke auf einem Server gespeichert werden, der sich in einem durch eine Einbruchanlage gesicherten Bereich befindet. Da heute bereits jeder Sachbearbeiter über einen eigenen Rechner verfügt und die Rechner untereinander vernetzt sind, sollte jede Dienststelle diese Sicherheitsmaßnahme einführen.

Ein besserer Schutz wäre natürlich zu erreichen, wenn die gesamte Dienststelle zusätzlich durch eine eigene Einbruchmeldeanlage geschützt wäre. Solche Anlagen können allerdings recht kostspielig werden, wenn sie ein größeres Gebäude wirksam schützen sollen. Hier wird man dann wohl einen Kompromiß eingehen müssen und lediglich die sensiblen Bereiche (wie Serverraum, Datenarchiv, Tresorraum) durch eine solche Anlage schützen. Gegen Einbrüche in das Gebäude, die auch ohne Diebstahl großen Schaden anrichten können, ist man dadurch jedoch nicht gefeit.

19.3.11 Funktelefone

Im Sommer 1997 wurde in verschiedenen Presseberichten auf ein neu entwickeltes, deutsches Gerät, den sog. IMSI-Catcher, aufmerksam gemacht. Mit diesem Gerät ist es möglich, den Standort von Mobiltelefonen zu ermitteln und Gespräche abzuhören, in dem es Schwachstellen in den Übertragungsprotokollen der Mobilfunktechnik (GSM = Global System for Mobile Communications, internationaler Standard für digitale zellulare Mobilfunknetze) ausnutzt. Der GSM-Standard wird auch in den in der Bundesrepublik verfügbaren Mobilfunknetzen verwendet. Diese Mobilfunknetze galten bis dahin allgemein als abhörsicher.

Die grundsätzliche Funktionsweise des IMSI-Catchers besteht darin, daß er eine legale Basisstation des jeweils ausgewählten Mobilfunknetzes simuliert und alle auf Empfang gestellten Mobilfunktelefone in seiner Reichweite zur Übermittlung ihrer IMSI/TMSI (IMSI = International Mobile Subscriber Identität, TMSI = Temporary Mobile Subscriber Identity), d. h. ihrer Benutzerkennung, auffordert. GSM-konform antworten die Mobiltelefone dieser stärksten (vermeintlichen) Basisstation und offenbaren dadurch, welche Benutzerkennungen sich zum jeweiligen Zeitpunkt in diesem geografischen Einzugsbereich aufhalten. Mobilfunktelefone, von denen ein Gespräch geführt wird, antworten nicht, so daß ein Umschalten auf ein laufendes Telefongespräch nicht möglich ist.

Durch eine andere Softwareversion und in Kombination mit einem weiteren Mobilfunktelefon kann bei einem Verbindungswunsch des abzuhörenden Mobiltelefons das Gespräch, für den Benutzer nicht erkennbar, über den IMSI-Catcher geleitet werden. Dazu fängt der IMSI-Catcher zunächst in der oben beschriebenen Weise das Mobiltelefon und veranlaßt dieses GSM-konform zur unverschlüsselten Datenübertragung, so daß der Gesprächsinhalt abhörbar ist.

Die Ursachen für die Funktionstüchtigkeit des IMSI-Catchers liegen in den Schwächen des

weltweiten GSM-Standards:

- Es erfolgt keine gegenseitige Authentifizierung zwischen Mobilfunktelefon und Basisstation. Eine Authentifizierung des Mobilfunktelefons geschieht erst nach Weiterreichen der Identifikationsdaten des Mobilfunktelefons an eine im Mobilfunknetz "weiter innen" liegende Schaltzentrale (MSC, Mobile Switching Center). Das Mobilfunknetz und seine Komponenten authentifizieren sich dem Mobilfunktelefon gegenüber überhaupt nicht, d.h. der Benutzer muß darauf vertrauen, mit seinem Mobilfunknetz über dessen Komponenten verbunden zu sein.
- Ob eine verschlüsselte Kommunikation erfolgt oder nicht, hängt technisch gesehen ausschließlich vom Mobilfunknetz, d.h. von der betreffenden Basisstation, ab. Dieses entscheidet, ob kryptiert wird oder nicht und "weist" das Mobilfunktelefon entsprechend an. Eine Einflußnahme durch den Mobilfunkteilnehmer ist nicht gegeben, eine Anzeige am Mobilfunktelefon "verschlüsselt/unverschlüsselt" ist nicht vorhanden. Nach Angaben der Netzbetreiber ist dies in dieser Form wegen der unterschiedlichen nationalen Regelungen zur Verwendung kryptografischer Methoden in Europa erforderlich und in der Bundesrepublik selbst soll die Kommunikation üblicherweise verschlüsselt erfolgen.

Wie im Arbeitspapier "Datenschutzfreundliche Technologien in der Telekommunikation" festgestellt wird, lagen die vorrangigen Zielsetzungen beim Aufbau der Mobilfunknetze in der Erbringung der geforderten Leistungen und in der funktionsgerechten Steuerung und Überwachung aller Aktivitäten für den Betreiber. Datenschutzfreundliche Techniken und mehrseitige Sicherheit haben bei der Systementwicklung keine Rolle gespielt. Nunmehr obliegt es den Betreibern, in geeigneter Form nachzubessern und es obliegt den Benutzern, derartige Nachbesserungen zu fordern.

Auf meine Nachfragen bei bayerischen Sicherheitsbehörden wurde erklärt, daß der IMSI-Catcher dort nicht eingesetzt wird.

19.3.12 Elektronische Steuererklärung (ELSTER)

In Abschnitt [21.3.6](#) meines 16. Tätigkeitsberichts (1994) bin ich auf ein Pilotverfahren des Bayer. Staatsministeriums der Finanzen eingegangen, bei dem Steuerklärungsdaten von der Lohnsteuerhilfe Bayern e.V. und von der DATEV e.G. auf elektronischem Weg an das Zentralfinanzamt übermittelt werden. Zur Datenübertragung wird der Telebox-400-Dienst der Deutschen Telekom AG bzw. das Übertragungsverfahren FTAM i.V.m. Wählleitungen benutzt. An diesem Verfahren können Steuerberater, die der DATEV e.G. angeschlossen sind, und die Beratungsstellen des Lohnsteuerhilfevereins Bayern e.V. teilnehmen. Eine unmittelbare Nutzung durch den Bürger ist mit diesen Verfahren nicht gegeben.

Bedingt durch die in den letzten Jahren

- drastisch gewachsene Anzahl an Personal Computern im Heimbereich,
- die breite Marktverfügbarkeit von Softwareprodukten zur Erstellung von Steuerklärungen und
- die Verbreitung des Internets mit seinen Möglichkeiten

verfolgt die Steuerverwaltung nun das Ziel, daß jedermann seine Steuererklärung direkt auch elektronisch übermitteln kann.

Bei dieser Fortentwicklung der Elektronischen Steuererklärung hat mich das Bayerische Staatsministerium der Finanzen leider nicht vorab beteiligt, so daß ich erst aus der Presse von dem Vorhaben erfahren habe und beim Bayerischen Staatsministerium der Finanzen schriftlich nachfragen mußte.

Im Rahmen des Projektes ELSTER erstellte die Steuerverwaltung einen Softwarebaustein, der in die kommerziell verfügbare Steuerklärungssoftware eingebaut werden kann und überließ diesen entsprechenden Softwareherstellern für einen Pilotversuch. Dieser Softwarebaustein druckt die Steuerklärung aus und veranlaßt die elektronische Datenübertragung an das Rechenzentrum der Steuerverwaltung. Zusätzlich zur elektronischen Übermittlung der Steuerklärung ist auch eine Steuerklärung in einer vereinfachten Form auf Papier abzugeben. Dies ist erforderlich, da für Steuerklärungen noch die eigenhändige Unterschrift gefordert wird (siehe hierzu [Nr.19.1.4](#), Einsatz kryptografischer Verfahren - Signaturgesetz) und auch notwendige Belege zur Steuerklärung eingereicht werden können.

Wie im bisherigen Verfahren mit der Lohnsteuerhilfe Bayern e.V. und der DATEV e.G. wird

eine sog. Telenummer auf der Steuerklärung aufgedruckt und auch den elektronisch übermittelten Daten mitgegeben. Dadurch ist eine zweifelsfreie Zuordnung der elektronischen zu den in Papierform vorliegenden Daten möglich.

Bevor die Daten vom privaten PC über Internet oder Wählleitung an die Steuerverwaltung abgeschickt werden, erfolgt eine durch den o.a. Softwarebaustein automatisch angestoßene kryptografische Verschlüsselung nach dem RSA/DES-Hybridverfahren. Im Rechenzentrum der Steuerverwaltung gelangen die übertragenen Daten zunächst in einen nicht vernetzten PC. Vor ihrer Weiterverarbeitung werden die Daten auf Viren geprüft und dechiffriert.

Im Rahmen einer Fortentwicklung ist daran gedacht, die Steuererklärung selbst als WWW-Formular im Internet zur Verfügung zu stellen, wodurch die Einbindung in ein Steuerklärungsprogramm entbehrlich würde.

Ergebnisse

Die Steuerverwaltung setzt ihre Bemühungen konsequent fort, die modernen IuK-Techniken zur weiteren eigenen Effizienzsteigerung und zu mehr Bürgerfreundlichkeit zu nutzen.

Dabei nutzt sie auch die Möglichkeiten der Kryptografie zur Sicherstellung der Vertraulichkeit bei der Datenübertragung über offene Netze und zur Sicherstellung der Datenintegrität. Den Aspekten der Authentizität und Zurechenbarkeit wird über die Zuordnung der elektronisch übermittelten Daten zu den in Papierform übermittelten Daten mittels der verwendeten Telenummer Rechnung getragen. Zum Schutz der Netzwerke der Steuerverwaltung vor unberechtigtem Zugriff von außen und vor Beschädigung durch Computerviren werden als Sicherheitsmaßnahmen ein einzelstehender PC als Kommunikations-PC und die Virenprüfung eingesetzt.

In Abhängigkeit

- von der Implementierung der Verschlüsselungsalgorithmen,
- von der verwendeten Schlüssellänge,
- von der Eineindeutigkeit der Erzeugung der Telenummer und
- von der Manipulationssicherheit des Softwarebausteins

hat die Steuerverwaltung - soweit erkennbar - alle derzeit verfügbaren Möglichkeiten ausgeschöpft, um eine datenschutzgerechte Lösung für die auch durch den Bürger selbst elektronisch übermittelte Steuererklärung zu ermöglichen.

19.3.13 Reinigung von Diensträumen und Aufbewahrung von Akten

Im Rahmen meiner technisch-organisatorischen Prüfungen stelle ich immer wieder fest, daß geeignete Behältnisse für die zugriffssichere Aufbewahrung von Akten mit personenbezogenem Inhalt nicht in ausreichendem Umfang zur Verfügung stehen. Ein unbefugter Zugriff Dritter, etwa durch Personal eines Reinigungsunternehmens, kann nicht ausgeschlossen werden. Dieses Thema war auch 1998 Gegenstand eines entsprechenden, letztlich abgelehnten Antrages mehrerer Abgeordneter an den Bayerischen Landtag.

Zur Lösung des Problems eröffnen sich eine Reihe von Möglichkeiten:

- Generelles Ziel sollte sein, in den jeweiligen Dienstzimmern eine ausreichende Anzahl an geeigneten Behältnissen zur zugriffssicheren Aufbewahrung dort benötigter schutzwürdiger Unterlagen bereitzustellen.
- Eine gewisse Entspannung der Situation läßt sich sehr häufig bereits dadurch erreichen, daß bei den Sachbearbeitern in den Diensträumen nur die jeweils unmittelbar benötigten Akten vorrätig sind.
- Für derart reduzierte Mengen reichen die verschließbaren Behältnisse in den Dienstzimmern dann häufig aus. Archive und Registraturen sind wie zentrale EDV-Räume meist ohnehin aus dem üblichen Reinigungsverfahren ausgenommen, so daß sich hier die Problematik eines unberechtigten Zugriffs durch Dritte so nicht stellt.
- Gelegentlich ist auch eine Form des Mischbetriebs mit eigenem und fremdem Personal bei der Durchführung der Dienstgebäudereinigung vorzufinden.
- Dabei sind besonders schutzwürdige Bereiche (z.B. Behördenleitung, Personalbereiche, Archive, DV-Räume) einer Reinigung durch eigenes Personal vorbehalten. Die übrigen Räume werden durch ein damit beauftragtes Unternehmen gereinigt.
- Sind vorübergehend keine der obigen Maßnahmen durchführbar und steht kein eigenes Personal für Reinigungsarbeiten (mehr) zur Verfügung, so sollte zumindest auf folgendes geachtet werden:
 - Die Reinigung besonders sensibler Bereiche soll nur innerhalb der Dienstzeit erfolgen, da dann eine Beaufsichtigung durch eigene Bedienstete möglich ist.
 - Das beauftragte Unternehmen soll schriftlich verpflichtet werden, immer nur dieselben Kräfte zur Reinigung des Dienstgebäudes einzusetzen.

- Die auftraggebende Behörde soll diese Reinigungskräfte gem. § 1 des Gesetzes über die förmliche Verpflichtung (Verpflichtungsgesetz) verpflichten.
- Nicht verpflichtete Reinigungskräfte können nur in nicht sensiblen Bereichen verwendet werden; in der Regel aber sollten sie stets verpflichtet werden
- Zur Kontrolle der Reinigungskräfte sollten Anwesenheitslisten geführt werden.

Sehr häufig wird angeführt, daß sich der Oberste Bayerische Rechnungshof in Abschnitt 16.1.1 seines Berichtes von 1990 für den Übergang von Eigenreinigung auf Fremdreinigung ausgesprochen habe. Dies ist zutreffend. Der Oberste Bayerische Rechnungshof hat aber auch darauf hingewiesen, daß es Bereiche geben kann, in denen aufgrund besonderer Sicherheitsanforderungen eine Eigenreinigung der Fremdreinigung vorzuziehen ist. Zu denken ist hier in erster Linie an den Finanz-, Sozial- und Justizbereich. In Krankenhäusern hat der Reinigungsdienst in der Regel keinen unbeobachteten Zugang zu Krankenakten.

Was die Beschaffung der erforderlichen Behältnisse betrifft, so verkenne ich nicht die Situation der Mittelknappheit in den öffentlichen Haushalten. Durch zeitliche Aufteilung der Beschaffungsmaßnahmen in Verbindung mit den oben erwähnten organisatorischen Maßnahmen bin ich jedoch überzeugt, daß sich eine datenschutzgerechte Lösung finden läßt.

19.4 Orientierungshilfen

19.4.1 Homepage des BayDSB

Mit Einrichtung einer eigenen Homepage ursprünglich auf dem Bayern-Server

(<http://www.bayern.de/dsb>) habe ich am 13.02.1997 meine Internet-Präsenz begonnen.

Es freut mich, daß bis heute, also im Zeitraum von knapp zwei Jahren, über 90.000 Zugriffe auf meine Homepage aus nahezu allen europäischen Ländern und auch aus anderen Kontinenten erfolgten. Dies bedeutet durchschnittlich ca. 3.900 Seitenabrufe pro Monat. Besonders nachgefragt wurden dabei die Rubriken "Datenschutz aktuell" (mit Presseerklärungen und Beiträgen zu aktuellen Themen und Fragen) und die Rubrik "Informationsmaterial" (zu technischen und organisatorischen Fragen). Darüber hinaus sind natürlich weitere interessante Rubriken, wie z.B. Tätigkeitsberichte, im Angebot.

Mit der Verlagerung meiner Dienststelle zum Bayerischen Landtag habe ich meine Homepage an das dortige Angebot äußerlich angepaßt und inhaltlich überarbeitet. **Sie ist nunmehr unter der Adresse "<http://www.datenschutz-bayern.de>" im Internet zu finden.** Hinweise und Anregungen nehme ich gerne entgegen.

19.4.2 Zusammenstellung der neuen Orientierungshilfen

Im Berichtszeitraum wurden in meiner Dienststelle folgende Orientierungshilfen neu erstellt bzw. überarbeitet:

- [Datensicherheit bei der Installation und beim Betrieb von Datenverarbeitungsanlagen - RM200, RM300, RM400, RM600, RM1000 - mit dem Betriebssystem SINIX/Reliant UNIX der Siemens Informationssysteme AG](#) (diese Orientierungshilfe wurde in Zusammenarbeit mit Mitarbeitern der Siemens Nixdorf Informationssysteme AG erstellt)
- [Sicherheitsbelehrung für die Benutzung von Personal Computern](#) (diese Orientierungshilfe ersetzt die bisherige Orientierungshilfe "Verpflichtungserklärung für PC-Benutzer")
- [Datensicherheit bei der Installation und beim Betrieb von Windows NT](#)

Der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder hat die Orientierungshilfe zu "[Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet](#)" vollständig überarbeitet und neu herausgegeben.

Diese Unterlagen können bei meiner Geschäftsstelle kostenlos angefordert werden und stehen auch auf meiner Homepage zum Abruf über das Internet zur Verfügung.

19.4.3 Werkzeug zum BSI-Grundschutzhandbuch

Im Abschnitt [18.4.1](#). meines 17. Tätigkeitsberichts war ich auf den Grundschutz im allgemeinen und das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) u.a. in Zusammenarbeit mit einigen Aufsichtsbehörden erstellte IT-Grundschutzhandbuch (IT-GSHB) eingegangen.

Das BSI stellt als Ziel des Grundschutzes dar, daß durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmaßnahmen ein grundlegendes Sicherheitsniveau für IuK-Systeme erreicht werden soll. Dieses erreichbare Sicherheitsniveau ist für einen mittleren Schutzbedarf angemessen und ausreichend. Da es sich dabei um die überwiegende Zahl der IuK-Systeme handeln dürfte, verringert sich durch die An-

wendung des IT-GSHB der Aufwand für die Erstellung des Sicherheitskonzeptes erheblich. Für IuK-Systeme mit höherem Schutzbedarf kann der Grundschatz als Ausgangsbasis dienen.

In den Jahren 1997 und 1998 wurde das IT-Grundschatzhandbuch überarbeitet. Es wurde u.a. um folgende Bausteine ergänzt:

- Häuslicher Arbeitsplatz
- Allgemeines nicht vernetztes IT-System
- Novell 4.x-Intranetware
- Heterogene Netze
- Elektronischer Datenaustausch per E-Mail
- LAN-Anbindung eines IT-Systems über ISDN
- Datenbanken
- Telearbeit

Da sich auch die Arbeit mit dem gedruckten IT-GSHB noch relativ zeitaufwendig gestaltete, beauftragte das BSI ein Unternehmen mit der Entwicklung und dem Vertrieb eines entsprechenden DV-gestützten Werkzeugs. Dieses Werkzeug, das BSI-Tool IT-Grundschatz, kann beim Bundesanzeiger-Verlag, Postfach 10 05 34, 50445 Köln, Tel: 0221/97668-200, Fax: 0221/97668-278, ISBN: 3-88784-853-5, bezogen werden. Die jährlich neu erscheinende Version des IT-GSHB kann mittels einer Importfunktion in das Tool importiert werden.

20. Der Beirat

Dem Beirat beim Landesbeauftragten für den Datenschutz gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den **Landtag**:

Mitglieder:		Stellvertretende Mitglieder:	
Franz Brosch	CSU	Prof. Dr. Hans Gerhard Stockinger	CSU
Joachim Herrmann	CSU	Johann Neumeier	CSU
Alfred Reisinger	CSU	Dr. Helmut Müller	CSU
Dr. Markus Söder	CSU	Markus Sackmann	CSU
Dr. Klaus Hahnzog	SPD	Dr. Thomas Jung	SPD
Franz Schindler	SPD	Joachim Wahnschaffe	SPD

ab 29.10.1998:		ab 29.10.1998:	
Franz Brosch	CSU	Prof. Dr. Hans Gerhard Stockinger	CSU
Petra Guttenberger	CSU	Johann Neumeier	CSU
Alexander König	CSU	Christian Meißner	CSU
Bernd Sibler	CSU	Thomas Obermeier	CSU
Dr. Klaus Hahnzog	SPD	Harald Güller	SPD
Franz Schindler	SPD	Joachim Wahnschaffe	SPD

Für den **Senat**:

Wolfgang Burnhauser	Hartwig Reimann
---------------------	-----------------

Für die **Staatsregierung**:

Hubert Kranz	Bayerisches Staatsministerium der Finanzen	Christian P. Wilde	Bayerisches Staatsministerium des Innern
--------------	--	--------------------	--

Der Bayerische Landesbeauftragte für den Datenschutz

18. Tätigkeitsbericht, 1998; Stand: 16.12.1998

Für die **Sozialversicherungsträger:**

Dr. Ludwig Bergner	Erster Direktor der LVA Oberbayern	Dr. Helmut Platzer	Stellvertretender Vorsitzender des Vorstandes der AOK Bayern
--------------------	------------------------------------	--------------------	--

Für die **Kommunalen Spitzenverbände:**

Klaus Eichhorn	Geschäftsleitender Direktor der AKDB	Hanns Herrlitz	Direktor bei der AKDB
		ab 05.01.1998: Wolfgang Kellner	AKDB

Für den **Verband Freier Berufe e. V.:**

Erwin Stein	Präsident der Steuerberaterkammer München	Dr. Wolf-Dieter Seeher	Zahnarzt
-------------	---	------------------------	----------

Den Vorsitz im Beirat führte Franz Brosch, MdL, sein Stellvertreter war Dr. Klaus Hahnzog, MdL.

Der Beirat tagte im vergangenen Berichtszeitraum acht Mal. Dabei befaßte er sich u.a. mit folgenden Themen:

- Beratung des 18. Tätigkeitsberichtes
- Datenübermittlung vom Sozialamt an die Polizei
- Speicherungen im Kriminalaktennachweis (KAN)
- Berichte von Datenschutzkonferenzen
- Einfügung eines neuen Art. 33 a in die Bayerische Verfassung (u.a. Wahl des Bayerischen Landesbeauftragten für den Datenschutz durch den Landtag)
- Veröffentlichung von Niederschriften öffentlicher Sitzungen des Gemeinderats im Internet
- Einführung von "Mißbrauchsermittlern" in der Sozialhilfe
- Verlängerung von Aufbewahrungsfristen nach den zum PAG ergangenen Verwaltungsvorschriften für Sexualstraftaten

Anlagen

Anlage 1: Entschließung der Datenschutzkonferenz vom 09./10. März 1995:

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z.B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten, sind Verkürzungen vorzunehmen.
3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bis-

herigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

Ergeht keine rechtskräftige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Er-
laß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Lösungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.
5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.
6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.
7. Für die Daten von Nebenbeteiligten (z.B. Anzeigerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.
8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 2: Entschließung der Datenschutzkonferenz vom 14./15.03.1996

Regelung der Öffentlichkeitsfahndung in Strafverfahren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt nachstehende Grundsätze für eine notwendige gesetzliche Regelung der öffentlichen Fahndung in Strafverfahren auf Basis der Vorlage des AK Justiz zustimmend zur Kenntnis.

Diese Grundsätze sollen schon jetzt soweit wie möglich bei der öffentlichen Fahndung beachtet werden (z.B. in den Fällen des § 131 StPO).

... (Protokollerklärungen mehrerer Datenschutzbeauftragter)

Grundsätze für die öffentliche Fahndung im Strafverfahren

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15.12.1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekanntem Tatverdächtigen, Beschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten ; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt, bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

- eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und
- der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Rest- freiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs.2 StrEG aufgenommen werden.

Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

Anlage3: Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22/23.10.1996

Maßnahmen zur Sicherung der Privatsphäre für den Fall der Einführung der akustischen Wohnraumüberwachung

1. Im Grundgesetz selbst ist festzulegen,
 - daß der Einsatz technischer Mittel zur Wohnraumüberwachung nur zur Verfolgung schwerster Straftaten, die im Hinblick auf ihre Begehungsform oder Folgen die Rechtsordnung nachhaltig gefährden und die im Gesetz einzeln bestimmt sind und
 - nur auf Anordnung eines Kollegialgerichts erfolgen darf.
2. Die Maßnahme darf sich nur gegen den Beschuldigten richten. Erfolgt ein Lauschangriff in der Wohnung eines Dritten, müssen konkrete Anhaltspunkte die Annahme rechtfertigen, daß sich der Beschuldigte in der Wohnung aufhält. In allen Fällen muß die durch Tatsachen begründete Erwartung vorliegen, daß in der überwachten Wohnung zur Strafverfolgung relevante Gespräche geführt werden.
3. Das Mittel der Wohnungsüberwachung darf nur angewandt werden, wenn andere Methoden zur Erforschung des Sachverhalts erschöpft oder untauglich sind. Bei einem Lauschangriff in Wohnungen dritter Personen bedeutet dies auch, daß die Maßnahme nur durchgeführt werden darf, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß ihre Durchführung in der Wohnung des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Täters führen wird.
4. Das Zeugnisverweigerungsrecht von Berufsheimlichkeitsgeheimnisträgern und Personen, die aus per-

sönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, muß gewahrt werden.

5. Die Dauer der Maßnahme wird zeitlich eng begrenzt. Auch die Möglichkeit der Verlängerung der Maßnahme ist zu befristen.
6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zu Beweis Zwecken noch als Ermittlungsansatz für andere als Katalogtaten zulässig. Personenbezogene Erkenntnisse aus dem Lauschangriff dürfen zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.
7. Wenn sich der ursprüngliche Verdacht nicht bestätigt, sind die durch den Lauschangriff erhobenen Daten unverzüglich zu löschen.
8. Die Betroffenen müssen unverzüglich und vollständig über die Durchführung der Maßnahme informiert werden, sobald dies ohne Gefährdung des Ermittlungsverfahrens möglich ist.
9. Eine Verfahrenssicherung durch den Zwang zur eingehenden Begründung und detaillierte jährliche Berichtspflichten der Staatsanwaltschaft für die Öffentlichkeit ähnlich den gerichtlichen Wire-Tap-Reports in den USA einschließlich einer Erfolgskontrolle ist vorzusehen. Anhand der Berichte ist jeweils - wegen der Schwere des Eingriffs - in entsprechenden Fristen zu überprüfen, ob die gesetzliche Regelung weiterhin erforderlich ist.
10. Die effektive Kontrolle der Abhörmaßnahmen und der Verarbeitung und Nutzung der durch sie gewonnenen Erkenntnisse durch Gerichte und Datenschutzbeauftragte ist sicherzustellen.

Anlage 4: Entschließung der Datenschutzkonferenz vom 17./18.04.1997

Beratungen zum StVÄG 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z.B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.
- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages "berechtigtes" statt eines rechtlichen Interesses gefordert.
- Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z.B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fan-

den in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag. Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:

- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.
- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.
- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.
- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.
- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.
- Speicherungs- und Lösungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.
- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

Anlage 5: Entschließung der Datenschutzkonferenz vom 17./18.04.1997

Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz -DNA-Analyse ("Genetischer Fingerabdruck")- die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungsmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die

genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z.B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81 e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

- Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafver-

folgung fördern kann.

- Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.
 - Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z.B. gestaffelt nach der Schwere des Tatvorwurfs).
3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.
 4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

Anlage 6: Entschließung der Datenschutzkonferenz vom 17./18.04.1997

Geplante Verpflichtung von Telediensteanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 (§ 5 Absatz 3) des Informations- und Kommunikationsdienste-Gesetzes vom 20.12.1996 - BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z.B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z.B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z.B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt. Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Diensteanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Anlage 7: EntschlieÙung der Datenschutzkonferenz vom 17./18.04.1997

Achtung der Menschenrechte in der Europäischen Union

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 zu den Dateien von Europol unterstützt werden soll.

Das Europäische Parlament hat in seiner EntschlieÙung zur Achtung der Menschenrechte gefordert, "alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen."

Anlage 8: Entschließung der Datenschutzkonferenz vom 17./18.04.1997

Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, daß in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z.B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z.B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibearbeiten an selbständige Schreibbüros.

Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), - z.B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.
3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen

wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, daß die personenbezogenen Patientendaten diesen Ärzten "in ihrer Eigenschaft als Arzt" bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmenschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist. Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Anlage 9: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20.10.1997 zu den Vorschlägen der Arbeitsgruppe der ASMK "Verbesserter Datenaustausch bei Sozialleistungen"

Verbesserter Datenaustausch bei Sozialleistungen

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich - insbesondere mit veränderten Verfahren der Datenerhebung - erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

- Datenerhebungen beim Betroffenen selbst
- Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben/Datenabgleich)

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z.B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritte erhalten keine Kenntnis von diesen Datenerhebungen.

Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z.B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz

der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, gehen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezugnehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

- 1. Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I)**

Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u.a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z.B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des

Betroffenen lassen diesen im unklaren, welche Daten wann an wen übermittelt wurden.

Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlaß erfolgen, abzulehnen sind.

Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften (zu D.I.1.1)

Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67a SGB X einholen, soweit das erforderlich ist.

Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

3. Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6)

Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebungen im Sozialbereich überhaupt

nicht ein.

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. Akzeptanz des Datenaustausches (zu E.IV)

Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, daß anlaßunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu

gesprächsbereit.

Anlage 10: Entschließung der Datenschutzkonferenz vom 23./24.10.1997

Novellierung des Bundesdatenschutzgesetzes (BDSG)

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschuß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z.B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;
- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;
- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;
- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z.B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;
- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft.

Dazu gehören insbesondere folgende Punkte:

- Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;
- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;
- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Videoüberwachung;
- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;
- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensibler Daten;
- Regelungen für Chipkarten-Anwendungen;
- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungregelung;
- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;
- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außer-

halb ihres Anwendungsbereichs verwenden darf;

- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;
- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Anlage 11: Entschließung der Datenschutzkonferenz vom 23./24.10.1997

Informationelle Selbstbestimmung und Bild- und Tonaufzeichnungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten ("Vermeidung kognitiver Dissonanzen"). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Video-

technologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z.B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.
2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.
3. Vorbehaltlich des o.g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z.B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Lösungsfristen.
4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt

werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.
6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

Anlage 12: Entschließung der Datenschutzkonferenz vom 23./24.10.1997

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptografische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die

Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm "Forschung und Entwicklung" aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Anlage 13: Entschließung der Datenschutzkonferenz vom 19./20. März 1998

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, daß bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, daß erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, daß auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen ("Free TV" und "Pay TV") muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, daß die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, daß so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;
- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;
- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veran-

staltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzerfordernungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

Anlage 14: Entschließung der Datenschutzkonferenz vom 19./20. März 1998

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen "Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten. Außerdem werden die Kundinnen und Kunden über diese "Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzzahlen in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Anlage 15: Entschließung der Datenschutzkonferenz vom 05./06.10.98

Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz – bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern – im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, daß sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, daß die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluß an ihren Beschluß der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten

Dateien

namentlich die

- Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;
- Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und –verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein "StVÄG 1996" erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Anlage 16: Entschließung der Datenschutzkonferenz vom 05./06.10.98

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellen Betroffene fest, daß sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert. Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Anlage 17: Entschließung der Datenschutzkonferenz vom 05./06.10.98

Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.
- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.
- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Anlage 18: Entschließung der Datenschutzkonferenz vom 05./06.10.98

Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, daß die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z.B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, daß die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

Anlage 19: Entschließung der Datenschutzkonferenz vom 05./06.10.98

Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlaß von Unsicherheiten ist. Sie weisen daher darauf hin, daß die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, daß Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Anlage 20: Entschließung der Datenschutzkonferenz vom 05./06.10.98

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlaß an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlaß an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.