Bayerischer Landtag
12. Wahlperiode

Drucksache **12/13933**

17. 12. 93

Fünfzehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1993

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 16

München, 17. Dezember 1993

An den
Präsidenten
des Bayerischen Landtags
Herrn Dr. Wilhelm Vorndran
München

Fünfzehnter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gem. Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes den fünfzehnten Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Inhaltsübersicht

1. Vorbemerkungen

1.1 Kontrolltätigkeit

Wie in den vergangenen Jahren lag auch im Berichtszeitraum 1993 einer der Schwerpunkte meiner Tätigkeit bei der **Überprüfung bayerischer Behörden.** Datenschutzkontrollen habe ich durchgeführt bei fünf Krankenhäusern, davon zwei Bezirkskrankenhäusern, einem Finanzamt, dem Landeskriminalamt, einem Polizeipräsidium, einer Polizeidirektion, einer Grenzpolizeiinspektion, dem Landesamt für Verfassungsschutz, einer Staatsanwaltschaft, einer Justizvollzugsanstalt, einem Landratsamt, zwei Regierungen, sechs Städten und Gemeinden, einer Universität, einem Gymnasium, zwei Schulämtern und einem Staatsarchiv. Hinzu kamen **technisch-organisatorische Kontrollen** bei 19 öffentlichen Stellen und Rechenzentren.

Ergänzt wurden die allgemeinen Kontrollen durch zahlreiche **Überprüfungen von Behörden aufgrund von Eingaben, Beschwerden und Presseberichten.** Besonders bedanken möchte ich mich wieder für die Mitarbeit der Bürger, die mich in ihren Eingaben auf Mängel im Datenschutz hinweisen und mir so die Möglichkeit verschaffen, gegen diese Mängel gezielt und mit entsprechender Breitenwirkung vorzugehen.

1.2 Situation des Datenschutzes in Bayern

Auf der Grundlage der durchgeführten Kontrollen und zahlreicher sonstiger Kontakte mit Behörden kann ich auch für das Berichtsjahr 1993 feststellen, daß der **Datenschutz in Bayern grundsätzlich gewährleistet** war. In einzelnen Bereichen aufgedeckte Mängel wurden von den kontrollierten Behörden in den meisten Fällen umgehend beseitigt. In einigen Fällen laufen noch Verhandlungen. Die Behörden waren in ihrer übergroßen Mehrzahl gegenüber den Anliegen des Datenschutzbeauftragten sehr aufgeschlossen. **Behindert wurde meine Kontrolltätigkeit lediglich bei einer Staatsanwaltschaft.**

Diese insgesamt positiven Feststellungen müssen allerdings vor dem Hintergrund **relativiert** werden, daß nach dem Datenschutzgesetz von 1978 in Bayern bisher nur Dateikontrollen zulässig waren. Akten können nur anläßlich von Dateikontrollen überprüft werden, um die Rechtmäßigkeit der Dateiverarbeitung zu überprüfen. Durch die gesetzlichen Beschränkungen der Datenschutzkontrolle in Bayern ist bisher ein Teil der Datenerhebung und -verarbeitung, gerade auch **in dem für die Freiheit der Bürger besonders bedeutsamen Bereich von Polizei, Staatsanwaltschaft und Verfassungsschutz, dem Landesbeauftragten für den Datenschutz nicht zugänglich.** Auch wenn ich über die gesetzlich eingeräumten Befugnisse hinaus aufgrund von Beschwerden etc. Kontrollen durchführen konnte, so sind mir doch Aussagen über die Situation des Datenschutzes außerhalb des Bereichs der Dateien praktisch nicht möglich. Zur Situation nach dem neuen Bayerischen Datenschutzgesetz verweise ich auf die Beiträge unter Nr. 1.4, 4.1.1, 5.2 und 6.3.

1.3 Inhalt und Schwerpunkte des 15. Tätigkeitsberichts

Den Schwerpunkt bilden wieder die Ergebnisse der durchgeführten **Datenschutzkontrollen,** die dabei gewonnenen **Erfahrungen** und die daraus gezogenen **Konsequenzen.** Zahlreiche **Zweifelsfragen** von Bürgern und Behörden bei der Auslegung und Anwendung des Datenschutzrechts waren wieder zu klären. Soweit die Stellungnahmen von allgemeinem Interesse sind, habe ich sie im Bericht wiedergegeben.

Zu einer Reihe von **Gesetzgebungsvorhaben,** Richtlinien und Dienstanweisungen, die den Datenschutz betreffen, habe ich Stellung genommen.

Bei der Novellierung des Bayerischen Datenschutzgesetzes habe ich nachhaltig auf die **Verankerung der verfassungsrechtlich gebotenen uneingeschränkten Kontrollkompetenz des Landesbeauftragten** für den Datenschutz über die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten der Bürger gedrängt. **Kontrollfreie Räume sind nicht hinnehmbar. „Vertrauen ist gut – Kontrolle ist besser!"** Dieser Erfahrungssatz gilt auch im demokratischen Rechtsstaat. Er gilt nicht nur für das Finanzgebaren, sondern genauso für das Informationsgebaren des Staates. Niemand würde auch nur daran denken, die Kontrolle des Obersten Rechnungshofs auf die automatisierte Finanzverwaltung zu beschränken. Auf die **negativen Auswirkungen der Einschränkungen** der Kontrollkompetenzen für den Datenschutz der Bürger gegenüber Justiz, Polizei und Verfassungsschutz wird im Bericht mehrfach hingewiesen.

Schwerpunkte im einzelnen:

- Im Vordergrund standen meine Bemühungen um einen **angemessenen Datenschutz im Sicherheitsbereich.** Allgemeine Querschnittskontrollen von **Dateien** ergaben in den meisten Fällen ein **hohes Datenschutzbewußtsein** bei Polizei und Verfassungsschutz und insgesamt einen hohen **Datenschutzstandard** beim Umgang mit personenbezogenen Daten. Es ist aber auch deutlich geworden, daß die Qualität der Datenverarbeitung von **Behörde zu Behörde recht unterschiedlich** ist und offensichtlich vom Ausbildungsstand und von der Sorgfalt der jeweiligen Sachbearbeiter abhängt.

  Neue Richtlinien für polizeiliche Datensammlungen, die vom Innenministerium erarbeitet wurden, werden unter der Ebene des Gesetzes künftig die **Grundlage für die Führung polizeilicher Datensammlungen** (Kriminalakten und sonstige Vorgänge) bilden. Bei der Abfassung der Richtlinien wurde ich rechtzeitig beteiligt. Mein Ziel war es dabei vor allem, daß nur solche Vorgänge in den landesweit abrufbaren Kriminalaktennachweis aufgenommen wer-

den, die der Polizei zur Erfüllung ihrer Aufgaben jederzeit verfügbar sein müssen, Vorgänge von lokalem Interesse hingegen nur in der Vorgangsverwaltung nachgewiesen werden (vgl. Nr. 4.1.3).

Die Datei **Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung,** die vor einigen Jahren entwickelt worden ist, ist nunmehr in datenschutzrechtlicher Hinsicht – von der noch fehlenden Protokollierung der einzelnen Datenabrufe abgesehen – weitgehend **ausgereift.** Personen, die wegen Wegfalls des Tatverdachts nicht mehr den Status Beschuldigter haben, aber zur Sachbearbeitung und Vorgangsverwaltung weiterhin gespeichert werden müssen, werden nicht mehr als Beschuldigte, sondern als Zeugen oder sonst neutral bezeichnete Personen geführt. In dieser Ausgestaltung stehen der Dienststelle die Vorgangsdaten für die Vorgangsverwaltung und die Sachbearbeitung, aber auch für die Verbrechensbekämpfung datenschutzgerecht zur Verfügung. Mit Nachdruck müssen allerdings die technischen Voraussetzungen für die **Protokollierung der Datenabrufe** geschaffen werden, damit dem Datenmißbrauch ein Riegel vorgeschoben wird (vgl. Nr. 4.10).

Die **Staatsfeinde-Datei APIS** befindet sich datenschutzrechtlich insgesamt in einem guten Zustand. Die **staatsfeindliche Zielsetzung** der als Beschuldigte oder Verdächtige gespeicherten Personen war in den meisten Fällen ohne weiteres **nachvollziehbar**. Künftig können hier auch **fremdenfeindliche Straftaten** zur effektiveren Bekämpfung des Rechtsextremismus erfaßt werden (vgl. Nr. 4.4.1).

- Im **Justizbereich** entspricht das bei den Staatsanwaltschaften eingesetzte automatisierte Verfahren zur Unterstützung der Geschäftsstellen grundsätzlich den datenschutzrechtlichen Anforderungen (vgl. Nr. 6.4.1).

  Während der Überprüfung der Datei traten allerdings Meinungsverschiedenheiten über den Umfang meiner Prüfungskompetenz bei der Kontrolle von Dateien zu Tage: **Der Landesbeauftragte für den Datenschutz wird bei seiner Kontrolltätigkeit behindert,** wenn ein anwesender Generalstaatsanwalt bei der Überprüfung der Richtigkeit einer Dateispeicherung – anstatt dem Landesbeauftragten die gesetzlich vorgesehene eigenverantwortliche Beiziehung von Akten zu erlauben – ihn nur am Ergebnis seiner Überprüfung „teilhaben" läßt (vgl. Nr. 6.3.2).

  Erneut habe ich mich **bei der Abfassung von Einstellungsbescheiden** der Staatsanwaltschaft für eine wesentlich stärkere Berücksichtigung des **Datenschutzes der Opfer von Straftaten** stark gemacht. Die Strafanzeige eines unbeteiligten Dritten, z. B. einer politischen Partei gegen den Betreiber eines Industriebetriebs, darf nicht dazu führen, daß hochsensible Gesundheitsdaten des Opfers der angeblichen Straftat dem Anzeigeerstatter mit der Möglichkeit der Weiterverbreitung mitgeteilt werden (vgl. Nr. 6.8.1).

  Wesentlich verbessert werden muß der Datenschutz bei der **Eintragung der Schuldunfähigkeit eines Beschuldigten in das Bundeszentralregister.** Wer beispielsweise wegen temporärer Schuldunfähigkeit in das Register eingetragen wird, muß hiervon benachrichtigt werden, damit er sich gegen ungerechtfertigte Nachteile wie etwa Eintragung auf Lebenszeit zur Wehr setzen kann. Eine Verbesserung hält auch das Justizministerium für notwendig (vgl. Nr. 6.8.5).

- Im Meldewesen bestehen keine datenschutzrechtlichen Bedenken gegen die **regelmäßige Weitergabe der Umzüge und Sterbefälle von den Meldeämtern an die Rundfunkanstalten,** damit diese die nicht angemeldeten Rundfunkteilnehmer zur Zahlung der Rundfunkgebühr anhalten können. Der Datenschutz ist **kein 15. Nothelfer für Schwarzseher und Schwarzhörer** (vgl. Nr. 8.8).

  Immer noch weitgehend unbekannt ist das Recht jedes Wahlberechtigten, der Weitergabe seiner **Adreßdaten an politische Parteien** und Wählergruppen zu widersprechen. Gerade im Superwahljahr 1994 sollten die Gemeinden die Bürger rechtzeitig auf ihr **Widerspruchsrecht** hinweisen.

- Bei der Einführung von **Autobahnbenutzungsgebühren** dürfen keine Abrechnungssysteme verwendet werden, bei denen von den Autobahnbenutzern **Bewegungsprofile** entstehen. Gleiches gilt für die Einführung von **Plastikkarten im öffentlichen Nahverkehr.** Zumindest wahlweise muß ein Zahlungsmodus, z.B. eine bezahlte Fahrkarte, zur Verfügung stehen, der die Entstehung von Bewegungsprofilen ausschließt (vgl. Nr. 17.3).

- An der **Produktion von Reality-TV-Sendungen** dürfen sich bayerische Behörden nur in Ausnahmefällen beteiligen, weil bei solchen Sendungen regelmäßig die Gefahr besteht, daß das Persönlichkeitsrecht der im Fernsehen gezeigten Opfer von Unfällen und Katastrophen erheblich verletzt wird. Hinnehmbar ist die Mitwirkung nur, wenn die Aufklärung der Bevölkerung und die Förderung der Hilfsbereitschaft eindeutig im Vordergrund stehen (vgl. Nr. 18.1).

1.4 Neues Bayerisches Datenschutzgesetz

Der Bayerische Landtag hat am 23. Juli 1993 das neue Bayerische Datenschutzgesetz beschlossen (GVBl. S. 498 ff.). Es tritt am 1. März 1994 in Kraft.

Wichtige begrüßenswerte Neuerungen im Datenschutz habe ich bereits im letzten Tätigkeitsbericht angekündigt: Es handelt sich im wesentlichen um die Einbeziehung der **Erhebung** von Daten sowie der Verarbeitung und Nutzung personenbezogener Daten in **Akten** in

das Gesetz, um Regelungen über die **Zweckbindung** erhobener Daten, über die Zulässigkeit von **Online**-Datenübermittlungen und über die Erweiterung des Rechts auf **Auskunft** über gespeicherte Daten. Die **Unabhängigkeit des Landesbeauftragten** für den Datenschutz wird durch das Gesetz gestärkt. Er soll künftig mit Zustimmung des Landtags für einen Zeitraum von 8 Jahren berufen werden und während dieser Zeit nur unter den Voraussetzungen abberufen werden können, die für die Amtsenthebung von Richtern auf Lebenszeit gelten. Auch kann er sich jederzeit an Landtag und Senat wenden. Der Datenschutzbeauftragte ist über die **Planung bedeutender Automationsvorhaben** zu informieren, sofern damit personenbezogene Daten verarbeitet werden. Die **Kontrollkompetenz** des Landesbeauftragten wird auf Akten ausgedehnt, **soweit ein konkreter Kontrollanlaß** vorliegt.

Einschränkung der Kontrollkompetenzen des Landesbeauftragten für den Datenschutz

Das neue Bayerische Datenschutzgesetz schränkt freilich die Kontrollkompetenzen des Landesbeauftragten für den Datenschutz und damit das Grundrecht auf informationelle Selbstbestimmung im Vergleich zu den meisten anderen Ländern – in einem Punkt sogar ohne Beispiel in Deutschland – in gravierender Weise ein. Zwar wird die Kontrollkompetenz in Bezug auf Akten erweitert. Die Erweiterung bleibt jedoch hinter dem nach meiner Auffassung verfassungsrechtlich gebotenen Umfang zurück.

Aufschub der Kontrolle der Datenerhebung bei Strafverfolgungsbehörden

Durch die Sondervorschrift des Art. 30 Abs. 4 wird die Kontrolle des Landesbeauftragten über die **Erhebung** von Daten durch Staatsanwaltschaft und Polizei bis zum Abschluß des Strafverfahrens **aufgeschoben.** Eine solche Beschränkung gibt es weder im Bundesdatenschutzgesetz noch in einem der anderen 15 Länderdatenschutzgesetze. Sie stellt eindeutig eine **Verschlechterung des Datenschutzes in Bayern dar.** Die Begründung der Staatsregierung hierfür genügt nicht.

Demgegenüber halte ich eine zeitnahe, nicht bis zum Abschluß des Strafverfahrens aufgeschobene externe Kontrolle der Datenerhebung gerade im Strafverfahren für unverzichtbar, insbesondere bei **tiefergehenden Eingriffen** in das informationelle Selbstbestimmungsrecht und bei **lange dauernden Strafverfahren,** in denen die Kontrolle zeitlich weit hinausgeschoben wird.

Beschränkung der Datenschutzkontrolle auf eine bloße Anlaßkontrolle

Durch die Sondervorschrift des **Art. 30 Abs. 1 Satz 2** wird die Kontrolle des Landesbeauftragten über die Erhebung und Verarbeitung von Daten, die ausschließlich in Akten enthalten sind, auf die bloße **Anlaßkontrolle** beschränkt. Dadurch wird die Datenschutzkontrolle insbesondere in den Bereichen erheblich erschwert, in denen der Bürger wegen verdeckter Tätigkeit der Behörden, insbesondere bei Staatsanwaltschaft und Polizei sowie beim Verfassungsschutz, in besonderer Weise des Schutzes einer unabhängigen Institution bedarf. Der Landesbeauftragte stößt hier im Aktenbereich auf Verletzungen des Datenschutzes nur durch blanken Zufall. Denn **der Bürger weiß von den verdeckten Maßnahmen nichts** und kann sich deshalb nicht an den Landesbeauftragten wenden. Dieser erfährt keine Anhaltspunkte und kann deshalb nicht wirksam tätig werden.

Effektive Datenschutzkontrolle und damit **effektiver Datenschutz** ist demgegenüber nur gewährleistet, wenn der Landesbeauftragte auch **ohne Anlaß gezielt** die Datenerhebung und Datenverarbeitung **im Aktenbereich** überprüfen kann. Die Beschränkung der Datenschutzkontrolle bei Daten, die allein in Akten enthalten sind, auf die bloße Anlaßkontrolle gibt es nur noch im Bund, in Baden-Württemberg und in Sachsen-Anhalt.

Datenschutz bei Datenerhebung und -verarbeitung für Begnadigungsverfahren

Auch gegen Art. 2 Abs. 4 BayDSG-neu hatte ich mich gewandt. Danach ist das Datenschutzgesetz nicht anwendbar auf die **Ausübung des Begnadigungsrechts.** Damit fehlt es für die Erhebung, Verarbeitung und Nutzung von Daten im gesamten Gnadenverfahren an einer gesetzlichen Grundlage. Auch die **Datenschutzkontrolle** über die Erhebung und Verarbeitung von Daten des Gnadenantragstellers und dritter Personen wird auf diese Weise **ausgeschlossen.**

Parlamentarische Behandlung

Meine Bemühungen, die Sondervorschriften Art. 30 Abs. 4 (Aufschub der Datenschutzkontrolle über die Datenerhebung im Strafverfahren), Art. 30 Abs. 1 Satz 2 (bloße Anlaßkontrolle bei der Erhebung und Verarbeitung von Daten in und aus Akten) und Art. 2 Abs. 4 (Ausschluß des Datenschutzgesetzes im Gnadenwesen) in der parlamentarischen Beratung noch zu verhindern, hatten leider keinen Erfolg.

1.5 10 Jahre Volkszählungsurteil des Bundesverfassungsgerichts

Als das Bundesverfassungsgericht am 15. Dezember 1983 im Urteil zum Volkszählungsgesetz das Grundrecht auf informationelle Selbstbestimmung aus der Taufe hob, sahen manche vielleicht ein **neues Zeitalter** anbrechen, in dem die Grenzen der Freiheit des Individuums gegenüber dem Staat ein bedeutendes Stück hinausgeschoben würden: Der Staat werde weniger Daten über die Bürger erheben, weniger Daten in seinen Dateien und Akten speichern, weniger Informationen austauschen und einen Großteil der Datenbestände vernichten.

Diese **euphorischen Hoffnungen** dürften nach den Erfahrungen des vergangenen Jahrzehnts inzwischen der Ernüchterung gewichen sein. Ein ehemaliger Datenschutzbeauftragter brachte dies mit folgendem Satz zum

Ausdruck: **„Die sieben fetten Jahre des Datenschutzes sind vorbei."**

Zwar ist das Grundrecht auf informationelle Selbstbestimmung heute von Gesetzgeber, Verwaltung und Gerichten **vorbehaltlos anerkannt.** Es bedarf keiner ausdrücklichen Verankerung im Grundgesetz. Jedem Bürger wird das Recht zugestanden, **grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.** Allerdings: Dieses Grundrecht kann, so das Bundesverfassungsgericht, im überwiegenden Allgemeininteresse durch Gesetze eingeschränkt werden, die freilich wiederum den Grundsätzen der **Normenklarheit** und der **Verhältnismäßigkeit** entsprechen und organisatorische und verfahrensmäßige **Vorkehrungen** treffen müssen, welche der Gefahr einer Verletzung des Persönlichkeitsrecht entgegenwirken.

Mit der Betonung des Gesetzesvorbehalts für jegliche Erhebung, Verarbeitung und Nutzung auch noch so unbedeutender personenbezogener Daten und der gleichzeitigen Hervorhebung der Grundsätze der Normenklarheit und Verhältnismäßigkeit hat das Bundesverfassungsgericht freilich im Bund und in den Ländern – wohl unbeabsichtigt – eine **Gesetzeslawine losgetreten,** die nach Zahl und Umfang der Artikel und Paragraphen in der Rechtsgeschichte ihresgleichen sucht. Ob diese Normenflut mit ihren **perfektionistischen** und **detaillistischen** Regelungen wirklich der Normenklarheit und der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und notwendig war, darf bezweifelt werden. Ebenso, ob diese Entwicklung das Recht dem Volk näher gebracht und verständlicher gemacht hat, ob sie **mehr informationelle Freiheit oder doch nur mehr Gesetze** gebracht hat. Denn nach 10 Jahren VZ-Urteil gibt es mehr und kompliziertere Gesetze als wie zuvor – wozu sicher nicht zuletzt die Datenschutzbeauftragten gerade unter Berufung auf das VZ-Urteil mit oft weit überzogenen Forderungen beigetragen haben. Es gibt aber auch nicht weniger, sondern mehr Datenspeicherungen.

Anzunehmen ist auch, daß die Effizienz der staatlichen Verwaltung bei der Bewältigung ihrer Aufgaben unter der Last perfektionistischer detaillistischer Regelungen gelitten hat und daß die Kreativität der Gesellschaft und ihre Fähigkeit zur Anpassung und Bewältigung der gegenwärtigen Herausforderungen durch enge, starre Gesetze gehindert wird. Diese Rechtsentwicklung war jedoch nicht die zwangsläufige Folge des VZ-Urteils, sondern sinnlose Übertreibungen haben dazu geführt.

Das VZ-Urteil läßt Einschränkungen des informationellen Selbstbestimmungsrechts im überwiegenden Allgemeininteresse zu. Im letzten Jahrzehnt, vor allem in letzter Zeit, haben die **Gefährdungen von Staat, Gesellschaft und jedes Einzelnen** erheblich zugenommen. Ich nenne nur die ernste Bedrohung durch den sprunghaften Anstieg der Alltags- und Gewaltkriminalität sowie durch neue Dimensionen der organisierten Kriminalität. Die innere Stabilität der Gesellschaft ist durch Werteverlust und den damit zusammenhängenden Verlust der Verbindlichkeit ethischer Normen gefährdet. Das Gleichgewicht zwischen der Freiheit des Einzelnen und seiner Bindung in der Gemeinschaft ist gestört. Übersteigerter Individualismus geht auf Kosten der Gemeinschaft. Egoismus und Rücksichtslosigkeit nehmen zu. Die sozialen Ressourcen werden knapp, aber ihr Mißbrauch häuft sich. Dies alles erfordert eine **neue Bewertung des Allgemeinwohls mit zwangsläufigen Auswirkungen auch für das Grundrecht auf informationelle Selbstbestimmung.** Das Volkszählungsurteil von 1983 steht einer solchen Neubewertung nicht im Weg. Es läßt Handlungsspielraum zur Bewältigung der Krise und bedarf keiner Revision.

1.6 Datenschutz – Innere Sicherheit – Organisierte Kriminalität

Der **Verfall der inneren Sicherheit** hat sich weiter beschleunigt. Die Zahl der registrierten Verbrechen in Deutschland ist 1992 gegenüber dem Vorjahr um über 600.000 (über 11 %) auf 6,29 Millionen angestiegen. Noch nicht einmal jedes zweite Delikt ist aufgeklärt worden. Die gefährliche Entwicklung der Alltags-, Gewalt- und organisierten Kriminalität kann zwar von Justiz und Polizei nicht allein aufgehalten werden. Ohne eine spürbare Steigerung der Effizienz ihrer Arbeit kann die Aufgabe aber keinesfalls gelöst werden. Dabei führt auch an der **Verbesserung der Fahndungsmöglichkeiten** der Strafverfolgungsbehörden zur raschen Aufklärung der Verbrechen und zur Aburteilung der Täter kein Weg vorbei.

Zur Bekämpfung der organisierten Kriminalität in Deutschland und Europa kann auf den **Einsatz von Observierungsmitteln in Wohnungen** („Großer Lauschangriff") keinesfalls verzichtet werden. Der Einsicht in diese Notwendigkeit versperren sich nur mehr wenige Bürger und Parteien. Zwar darf man sich von diesem Fahndungsmittel keine Wunderdinge erwarten. Es ist aber als Teil eines Sicherheitspakets notwendig, damit die Strafverfolgungsbehörden zu den Zentren verbrecherischer Organisationen vordringen können. Verbrechensbekämpfung darf auch nicht nach dem Motto betrieben werden: „Die Kleinen (Ganoven) fängt man, die Großen läßt man laufen."

1.7 Persönlichkeitsschutz im Bayer. Petitionsgesetz

Der Bayer. Landtag hat am 17. Juni 1993 das Bayer. Petitionsgesetz beschlossen. Art. 6 enthält unter den Regelungen zur Aufklärung des Sachverhalts auch Bestimmungen zum Schutz personenbezogener Daten.

Dabei hatte der Landtag sachgerecht abzuwägen zwischen seinem **Informationsbedürfnis,** wenn er sich mit einer Petition befaßt, und dem **Schutzbedürfnis** des Petenten und betroffener dritter Personen.

Für die **Übermittlung** personenbezogener Daten durch die Staatsregierung an den Landtag bestimmt das Gesetz, daß die Vorschriften über den Schutz von Geheimnissen und von personenbezogenen Daten zu beachten sind.

- Daten des Petenten selbst können dem Landtag übermittelt werden, wenn dies zur sachlichen Behandlung und Verbescheidung erforderlich ist.
- Sind in den Unterlagen mit solchen Daten **weitere Daten** des Petenten oder **Daten Dritter** so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht offensichtlich überwiegende schutzwürdige Interessen des Petenten oder Dritter entgegenstehen.
- Die Übermittlung personenbezogener Daten **Dritter,** die zur sachlichen Behandlung und Verabschiedung der Petition erforderlich sind, ist zulässig, soweit nicht offensichtlich überwiegende schutzwürdige Interessen der Dritten entgegenstehen.

Zum **Umgang** mit übermittelten personenbezogenen Daten im Landtag bestimmt das Gesetz:
Über die **Geheimhaltung** der übermittelten personenbezogenen Daten muß der Ausschuß jeweils entscheiden. Faßt er einen **Geheimhaltungsbeschluß,** so dürfen die Daten nur in anonymisierter Form für weitere parlamentarische Zwecke verwendet werden. Wenn die Geheimhaltung von Daten durch ein Gesetz ausdrücklich vorgeschrieben ist, ist die Angelegenheit in nichtöffentlicher Sitzung zu behandeln.

Im Gesetzgebungsverfahren habe ich dem Landtag Vorschläge zur besseren Berücksichtigung des Persönlichkeitsrechts im Petitionsverfahren unterbreitet. Sie wurden im wesentlichen berücksichtigt. Über meine Vorschläge zur Ergänzung der Geschäftsordnung des Bayer. Landtags durch eine Regelung über den Ausschluß der Öffentlichkeit (§ 29) zum Schutz des Persönlichkeitsrechts Betroffener bei den Beratungen des Plenums und der Ausschüsse hat der Landtag noch nicht entschieden.

1.8 Entwurf einer EG-Datenschutzrichtlinie

Die Europäische Union bereitet eine Datenschutzrichtlinie vor, deren Ziel es ist, den Schutz der Rechte und Freiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Der freie Verkehr personenbezogener Daten zwischen den Mitgliedsstaaten soll allerdings aus Gründen des Datenschutzes nicht beschränkt oder untersagt werden.

Der überarbeitete Richtlinienentwurf stellt aus der Sicht des Datenschutzes eine erhebliche Verbesserung gegenüber dem ersten Entwurf dar. Die Datenschutzbeauftragten des Bundes und der Länder haben sich zu dem geänderten Richtlinienvorschlag der EG-Kommission in einem Beschluß vom 16. und 17. Februar 1993 geäußert (Anlage 1).

2. Gesundheitswesen

Schwerpunkt meiner Tätigkeit im Gesundheitswesen war die datenschutzrechtliche Prüfung von **Krankenhäusern,** darunter zwei Bezirkskrankenhäuser. Die Diskussion um den Datenschutz bei **Krebsregistern** habe ich mit Stellungnahmen zu einem Entwurf für ein Bundeskrebsregistergesetz und mit der Beratung von Krankenhäusern fortgesetzt, die sich dem bayerischen Konzept der klinischen Krebsregister anschließen wollen. Die **Beratung medizinischer Forschungseinrichtungen** über die Einhaltung des Datenschutzes bei der Durchführung wissenschaftlicher Forschungsprojekte hat sich ausgeweitet.

2.1 Prüfung von Krankenhäusern

Im Berichtszeitraum habe ich datenschutzrechtliche Kontrollen bei zwei Krankenhäusern, zwei Bezirkskrankenhäusern sowie bei der Patientenverwaltung eines Klinikums durchgeführt. Gegenstand der Kontrollen waren **Dateien** und **Karteien** sowie im Hinblick auf die Nutzung und Übermittlung von Patientendaten aus Dateien oder Karteien (Art. 27 Abs. 4 und 5 BayKrG) **ausgewählte Aktenunterlagen** der Krankenhausverwaltung. Hingegen wurden Datenspeicherungen und -übermittlungen im medizinischen Bereich in bzw. aus den Krankengeschichten nicht geprüft. Bei den Kontrollen wurden **keine gravierenden Mängel** entdeckt. Insbesondere in den Bezirkskrankenhäusern war bei den Ärzten und dem übrigen Klinikpersonal ein hohes Maß an Sensibilität für den Schutz der Patientendaten festzustellen.

In folgenden Punkten sind aus datenschutzrechtlicher Sicht noch **Verbesserungen notwendig:**

- **Zu viele Daten an die gesetzlichen Krankenkassen**

  Die Krankenhäuser sind verpflichtet, bei einer Krankenhausbehandlung den gesetzlichen Krankenkassen die in § 301 SGB V aufgezählten Angaben zu übermitteln. Die geprüften Krankenhäuser übermittelten teilweise jedoch auch Daten, die über die in dieser Vorschrift aufgezählten Angaben hinausgehen. Dies resultiert meist daraus, daß die Daten, die bei der Aufnahme für Zwecke des Krankenhauses erfragt werden, ohne Rücksicht auf die Einschränkungen des § 301 SGB V an die Krankenkasse weitergegeben werden. Daten, deren Weitergabe nicht durch § 301 SGB V gedeckt ist, müssen bei der Aufnahmeanzeige an die Krankenkasse unterdrückt werden, soweit sie den Krankenkassen nicht ohnehin bekannt sind.

- **Auskunft über Klinikaufenthalt an Besucher**

  Insbesondere den Bezirkskrankenhäusern stellt sich die Frage, ob sie an der Pforte oder telefonisch Auskunft über den Aufenthalt eines Patienten geben dürfen. Bei den geprüften Bezirkskrankenhäusern wurde vom Patienten keine Einwilligung in die Auskunft eingeholt. Auskunft über den Aufenthalt des

Patienten wurde nur dann nicht erteilt, wenn es der Patient von sich aus wünschte.

In Bezirkskrankenhäusern besteht die Schwierigkeit bei der Einholung einer Einwilligung darin, daß lediglich ca. zwei Drittel der Patienten in der Lage sind, die Frage zu beantworten, ob sie Einwände gegen eine Auskunftserteilung an Dritte haben. Auch wenn man diese schwierige Situation berücksichtigt, halte ich es doch gerade bei Bezirkskrankenhäusern für notwendig, nach Möglichkeit schon im Aufnahmegespräch durch **ausdrückliches Befragen** festzustellen, ob Einverständnis mit der Pfortenauskunft besteht. Es sind viele Fälle vorstellbar, in denen Patienten nicht wünschen, daß Besuchern Auskunft über ihren Aufenthalt im Bezirkskrankenhaus erteilt wird.

Ich habe den Bezirkskrankenhäusern folgende Lösung vorgeschlagen:

Von Patienten, bei denen der aufnehmende Arzt davon ausgehen kann, daß sie die Frage verstehen und beantworten können, ist die **Einwilligung** in die Erteilung der Auskunft über ihren Aufenthalt einzuholen. Es empfiehlt sich, die Patienten zu fragen, ob Einwände dagegen bestehen, daß Auskunft über ihren Aufenthalt an Angehörige bzw. nahestehende Personen sowie an dritte Personen gegeben wird.

Bei Patienten, die nicht in der Lage sind, ihr Einverständnis zu erteilen, ist die Zustimmung zur Auskunft gegenüber **Angehörigen** zu unterstellen, solange nicht nach den Umständen das Gegenteil anzunehmen ist. Dagegen kann nicht davon ausgegangen werden, daß sich die mutmaßliche Einwilligung auch auf eine Auskunftserteilung gegenüber **Dritten** erstreckt. Die Frage nach der Auskunftserteilung sollte jedoch schnellstmöglich nachgeholt werden, sobald der Patient dazu gesundheitlich in der Lage ist. Ggf. muß der gesetzliche Vertreter hierüber entscheiden.

Für den Pförtner muß mit einem Blick erkennbar sein, ob und in welchem Umfang eine Auskunft zulässig ist. Dies sollte am Bildschirm angezeigt werden. Zur Lösung des Problems ist ein Arbeitskreis der bayerischen Bezirke eingesetzt.

2.2 Datenschutzberatung bei Forschung mit Patientendaten

Immer wieder holen medizinische Forschungseinrichtungen meine Stellungnahme zu Datenschutzfragen bei Forschungsvorhaben ein. Meist handelt es sich um Fragen der **Anonymisierung** von Patientendaten oder um den datenschutzgerechten **Zugang zu Patientendaten von Krankenhäusern.**

Anonymisierung

Wenn Krankenhäuser für Forschungszweeke **anonymisierte Patientendaten** zur Verfügung stellen sollen, genügt es in der Regel nicht, Namen und Anschrift des Patienten wegzulassen. Auch unter den verbleibenden Daten können Informationen sein, die eine Identifizierung einzelner Patienten erlauben. Auf das mögliche **Zusatzwissen** der Personen, welche die Daten erhalten, kommt es in diesem Zusammenhang besonders an.

Ein **Identifizierungsrisiko** enthält in der Regel das Geburtsdatum. Statt dessen sollten möglichst **Altersgruppen** gebildet werden. Die Angabe von Geburtstag und -monat sollte jedenfalls unterbleiben. Andere Angaben können z.B. auch in Kombination mit weiteren Daten eine Identifizierung erleichtern. Dazu gehören beispielsweise Familienstand, Ausbildung, berufliche Stellung, Wohngemeinde und Postleitzahl. Vor allem die neuen sehr detaillierten Postleitzahlen können zu deutliche Hinweise auf bestimmte Personen geben.

Ein erhebliches Identifizierungsrisiko ist regelmäßig in **Freitextfeldern** oder -zeilen zu sehen, insbesondere wenn dort „Sonstiges" eingetragen werden soll. Hier können unabsichtlich Hinweise gegeben werden, die einzelne Personen unmittelbar oder mit geringem Zusatzwissen bestimmbar machen. Den Personen, die solche Freitextfelder ausfüllen, müssen daher möglichst **klare Vorgaben** gemacht werden, damit keine identifizierenden Hinweise eingetragen werden.

Zugang zu Patientendaten

Der Zugang zu Patientendaten aus Krankenhausunterlagen wird in Bayern in manchen Fällen durch Art. 27 des Bayer. Krankenhausgesetzes ermöglicht. Nach Art. 27 Abs. 4 Satz 1 und 2, insbesondere Satz 2, 2. Halbsatz dürfen **in beschränktem Umfang** auch **externe Forscher** im Krankenhaus ohne Einwilligung Patientendaten für wissenschaftliche Forschungsvorhaben aus Patientenakten heraussuchen. **Voraussetzung** hierfür ist, daß sich das Krankenhaus den Forschungszweck zu eigen macht, etwa weil die Verwirklichung des Forschungsvorhabens einem **Forschungsinteresse des Krankenhauses** entspricht. Das Forschungsinteresse des Krankenhauses muß schriftlich festgehalten werden. Auch bei solchen, von außen an das Krankenhaus herangetragenen Forschungsvorhaben sind jedoch grundsätzlich **zunächst Krankenhausärzte und Krankenhauspersonal** zur Auswertung der Patientenunterlagen einzusetzen. Ist dies jedoch, etwa wegen der Umfänglichkeit der Erhebung, nicht möglich, so erlaubt die Vorschrift eine Tätigkeit krankenhausfremder Forscher **im Krankenhaus.** Externe Forscher müssen zur **Verschwiegenheit verpflichtet** werden. Diesbezügliche Erklärungen können durch **Vertragsstrafenversprechen** zusätzlich abgesichert werden. Dies gilt auch dann, wenn im Einzelfall daneben eine strafbewehrte Schweigepflicht bestehen sollte. Ferner müssen die **personenbezogenen** Daten im **Gewahrsam** des **Krankenhauses** verbleiben. Hierdurch wird sichergestellt, daß die für die Forschung erhobenen Daten **nur** in bereits **anonymisierter Form den Schutzbereich des Krankenhauses verlassen.**

Zugang zu Daten aus Todesbescheinigungen

Für manche Forschungsvorhaben wäre auch der Zugang zu den Daten in Todesbescheinigungen (Leichenschauscheinen), die von den Gesundheitsämtern aufbewahrt werden, von Wichtigkeit. Dies gilt beispielsweise für die Datensammlung der bayerischen klinischen Krebsregister. Es ist zu hoffen, daß hierfür in nächster Zeit eine Erlaubnis durch eine Ergänzung des **Bayer. Bestattungsgesetzes** geschaffen wird. Zu ersten Überlegungen für einen solchen Gesetzentwurf habe ich Stellung genommen. Über Einzelheiten ist nach der Einbringung in den Landtag zu berichten.

2.3 Zentrale zur Weiterverlegung von Patienten

Im 14. Tätigkeitsbericht habe ich darüber berichtet, wie die Zentrale zur Weiterverlegung von Patienten (ZWv), die von der Landeshauptstadt München eingerichtet worden ist, mit der Erhebung und Verarbeitung von Patientendaten zusammenhängende Datenschutzfragen gelöst hat. Die ZWv vermittelt die Weiterverlegung von Patienten aus teuren, für sie nicht mehr benötigten in kostengünstigere Intensivbetten, damit die besonders hochwertigen Behandlungsmöglichkeiten möglichst schnell wieder für Akutfälle verfügbar sind.

Offengeblieben war damals die Frage, ob der **Umfang** der von den Intensivstationen zur ZWv weitergeleiteten Patientendaten auf das erforderliche Maß beschränkt ist. Auf meine Bitte hat die Zentrale das Datenerhebungsformular zweimal überarbeitet und nunmehr einen Datensatz festgelegt, der auf den zur ordnungsgemäßen Weiterverlegung von Patienten erforderlichen Umfang beschränkt ist. Da hier Neuland betreten wurde, konnte der korrekte Umfang dieses Datensatzes nur durch kritische Begleitung der ersten Praxismonate gefunden werden.

2.4 DV-Projekt für Staatliche Gesundheitsämter

Bei einem staatlichen Gesundheitsamt wurde ein Verfahren zur DV-Unterstützung der staatlichen Gesundheitsämter entwickelt. Technisch-organisatorische Fragen des Datenschutzes bei diesem Projekt sind im 14. Tätigkeitsbericht unter Nr. 20.2.2 angesprochen. Aus rechtlicher Sicht habe ich aus der vorgelegten Verfahrensbeschreibung den **Speicherungsumfang** und die **interne Abschottung** im Gesundheitsamt gemäß Art. 6 des Gesundheitsdienstgesetzes (GDG) geprüft.

Speicherungsumfang

Das DV-Verfahren ist ein Aktenauffindungssystem. Es speichert über jeden Besucher des Gesundheitsamtes Daten, die bei einem späteren Besuch ein **Wiederauffinden** früher angelegter Akten und den Ausdruck von **Statistiken** erlauben. Außerdem werden Schreibarbeiten durch **Textautomation** unterstützt. Gegen den Umfang der vorgesehenen Datenspeicherung bestanden bei der Pilotanwendung keine Einwände.

Interne Abschottung

Zur Sicherstellung des in Art. 6 GDG festgelegten **Verwertungsverbots** müssen **organisatorische Abschottungsmaßnahmen** getroffen werden. Für das DV-System ergeben sich daher folgende Anforderungen:
Das DV-System darf keine Angaben über gesundheitliche Probleme, die das Gesundheitsamt bei **freiwilliger Beratung** oder **freiwilliger Begutachtung** erfahren hat, für die Sachbearbeitung außerhalb dieser Tätigkeit zur Verfügung stellen, z.B. am Bildschirm anzeigen. Die Art der Erkrankung, die bei freiwilliger Beratung oder Begutachtung bekannt wurde, darf am Bildschirm nur den für diese freiwillige Beratung und Begutachtung zuständigen Mitarbeitern angezeigt werden. So darf dem für die hoheitliche Seuchenbekämpfung zuständigen Mitarbeiter auf dem Bildschirm nicht angezeigt werden, wegen welcher gesundheitlicher Probleme ein vor ihm sitzender Besucher sich früher bereits hat freiwillig untersuchen oder begutachten lassen. Hingegen ist die Anzeige lediglich der Nummern der Sachgebiete, die sich in freiwilliger Beratung oder Begutachtung mit dem Besucher befaßt haben, auf dem Bildschirm des hoheitlich tätigen Mitarbeiters unbedenklich, solange die Sachgebietsnummern so vergeben sind, daß sie nicht inzidenter auf ein bestimmtes gesundheitliches Problem hinweisen.

Diese Anforderungen waren beim Pilotverfahren erfüllt. Nach der vorgelegten Verfahrensbeschreibung werden den Mitarbeitern für die Sachbearbeitung am Bildschirm nur **die Aktenzeichen ihres eigenen Sachgebiets vollständig** angezeigt. Soweit zu Betroffenen auch in **anderen Sachgebieten** Unterlagen vorhanden sind, wird lediglich die betreffende Sachgebietsnummer, jedoch kein Hinweis auf bestimmte gesundheitliche Probleme angezeigt. Der Mitarbeiter kann sich mit dem angezeigten Sachgebiet in Verbindung setzen. Dieses muß nach Maßgabe des Art. 6 GDG entscheiden, ob und in welchem Umfang aus seinen Unterlagen über freiwillige Beratung oder Begutachtung Daten für die anderen Zwecke des anfragenden Sachgebiets zur Verfügung gestellt werden können. Mit dem Besucher kann abgeklärt werden, ob er mit der Beiziehung der Unterlagen aus freiwilliger Beratung oder Begutachtung einverstanden ist.

Die Sachgebiete sind beim geprüften Gesundheitsamt durch Zusammenfassen verschiedener Gegenstände so definiert, daß die einzelnen Sachgebietsnummern keine bestimmten Arten von Erkrankungen aus der freiwilligen Beratung oder Begutachtung erkennen lassen.

Vor dem Einsatz des Systems bei **anderen Gesundheitsämtern** muß jeweils geprüft werden, ob dort die Sachgebiete so festgelegt sind, daß durch die Bildschirmhinweise auf andere Sachgebiete, bei denen weitere Vorgänge vorhanden sind, etwa den Sachbearbeitern im Hoheitsbereich nicht mehr Informationen angezeigt werden, als im Hinblick auf die organisatorische Sicherung des Verwertungsverbots des Art. 6 GDG zulässig ist.

2.5 Entwurf eines Bundeskrebsregistergesetzes

Gegenüber dem Staatsministerium des Innern habe ich mich zu einem Entwurf für ein Bundeskrebsregistergesetz geäußert.

Nachdem in Bayern erfolgreiche Schritte unternommen wurden, auf der Basis von klinischen Krebsregistern auch wichtige epidemiologische Daten zu sammeln, sollte nach meiner Auffassung ein Bundeskrebsregistergesetz neben dem im Entwurf vorgesehenen zentralen Register auch andere Modelle zulassen wie beispielsweise die **bayerische klinische Konzeption,** die bei der Krebsbehandlung zusätzliche Vorteile bietet, oder das baden-württembergische dezentrale Verschlüsselungsmodell. Auch Möglichkeiten der Kombination klinischer Datensammlungen mit einem landeszentralen statistischen Krebsregister sollten offen bleiben. Ein Bedürfnis nach einer bundesgesetzlichen Regelung besteht nur für die Festlegung einheitlicher Datensätze und für die Regelung der Datenweiterleitung an eine bundeszentrale Stelle. Im übrigen sollte aber die Wahl und Ausgestaltung der Registermodelle, insbesondere die datenschutzrechtliche Ausgestaltung, den Ländern überlassen bleiben.

Bei einem landeszentralen behandlungsunabhängigen statistischen Register, das bisher außerhalb Bayerns favorisiert wird, ist die **Anonymisierung** der gespeicherten Daten wichtig. Der Gesetzentwurf sah zu diesem Zweck eine **Vertrauensstelle** vor, welche die Patientendaten von den Kliniken und niedergelassenen Ärzten personenbezogen erhält und verschlüsselt, sowie eine **Registerstelle,** welche die von der Vertrauensstelle gelieferten verschlüsselten Daten speichert. Für die Verbesserung der Anonymisierung der gemeldeten Daten habe ich Vorschläge unterbreitet.

Nach dem Gesetzentwurf soll die Vertrauensstelle, die noch personenbezogene Patientendaten zu sehen bekommt, unter **ärztlicher Leitung** stehen. Damit sollen die durch § 203 Abs. 1 Nr. 1 des Strafgesetzbuches garantierte ärztliche Schweigepflicht sowie das Zeugnisverweigerungsrecht und das Beschlagnahmeverbot auf die Vertrauensstelle ausgeweitet werden. Die Festschreibung der „ärztlichen Leitung" genügt jedoch nach überwiegender Ansicht für einen solchen Schutz nicht. Zum Schutz der Patientendaten vor Zweckentfremdung, insbesondere vor Inanspruchnahme als Beweismittel, muß das Beschlagnahmeverbot im Bundesgesetz selbst festgelegt werden.

2.6 HIV-Test bei Risikogruppen

Wie einem Zeitungsbericht zu entnehmen war, warnte der Bundesdatenschutzbeauftragte in Zusammenhang mit der Praxis, alle Blutspenden generell einem HIV-Test zu unterziehen, davor, bestimmte **Risikogruppen** wie Drogenabhängige oder Prostituierte einem **Zwangstest** unterziehen zu wollen. Solche Zwangstests bedürften einer ausdrücklichen rechtlichen Ermächtigung, schließlich handle es sich um einen Eingriff in die körperliche Unversehrtheit.

Hierzu habe ich der Zeitung mitgeteilt, daß es jedenfalls für bayerische Gesundheitsbehörden nicht an einer ausreichenden Rechtsgrundlage für Zwangstests fehle. In Bayern werde die Gefahr der HIV-Infektion durch Risikogruppen seit Mitte der 80er Jahre entschieden ernster beurteilt als etwa durch das Bundesgesundheitsamt oder den Bundesdatenschutzbeauftragten. Deshalb würden die vorhandenen Rechtsgrundlagen ausgeschöpft.

Am 25. Februar 1987 hat die Staatsregierung einen umfassenden Katalog von Maßnahmen zur Bekämpfung von Aids beschlossen. In der Bekanntmachung vom 19. Mai 1987 hat das Staatsministerium des Innern hierzu Hinweise für den Vollzug des Seuchen-, Polizei- und Ausländerrechts gegeben. Die bayerischen Maßnahmen haben ihre **Rechtsgrundlage im geltenden Bundesseuchengesetz.** Die Maßnahmen sehen u.a. vor: Männliche und weibliche Prostituierte sowie intravenös Drogenabhängige (Fixer) gelten als „ansteckungsverdächtig" im Sinne des Bundesseuchengesetzes. Sie werden vierteljährlich vom Gesundheitsamt zu einem HIV-Antikörper-Test vorgeladen. Die Vorladung erfolgt zunächst formlos. Wird ihr nicht Folge geleistet, so wird die betreffende Person förmlich **vorgeladen** und kann – im Weigerungsfalle – auch von der Polizei **vorgeführt** werden. Läßt sich der Ansteckungsverdacht im Gespräch mit dem Amtsarzt nicht ausräumen, so wird ein HIV-Antikörper-Test durchgeführt. Nur im Falle der Weigerung wird die hierfür erforderliche Blutentnahme zwangsweise vorgenommen.

Es gibt also bereits Schutzvorschriften gegen die Ausbreitung von Aids durch Risikogruppen wie Drogenabhängige oder Prostituierte. Man muß diese Schutzvorschriften nur anwenden. Datenschutz ist jedenfalls **keine Entschuldigung für tatenloses Zusehen.**

2.7 HIV-Test bei allen Blutuntersuchungen?

Der Bundesgesundheitsminister hat nach Presseberichten ein Gesetz gefordert, wonach bei **allen Blutuntersuchungen in Kliniken und Arztpraxen ein HIV-Test durchgeführt wird,** wenn der Betroffene **nicht widersprochen** hat. Nach der Information des Patienten über das Testergebnis sollten die Daten **anonym verarbeitet** werden. Durch die Unterrichtung der Betroffenen würden viele Infizierte wesentlich früher gewarnt und damit über ein Ansteckungsrisiko informiert, das von ihnen ausgehen kann. Die Testergebnisse sollten anonym zu Statistiken verarbeitet werden, die wegen der hohen Zahl der Tests aussagefähiger wären als die bisherigen aus der anonymen Laborberichtspflicht gewonnenen Statistikdaten. Durch Zahlencodes sollten Doppelmeldungen ausgeschlossen werden.

Dieses Vorhaben muß aus **Datenschutzsicht noch gründlich geprüft werden.** Vorläufig läßt sich feststel-

len, daß die Berücksichtigung von Widersprüchen gegen HIV-Tests die datenschutzrechtliche Problematik entschärft.

Bisher werden HIV-Tests nicht generell bei jeder Blutentnahme durchgeführt. Soweit bekannt, holen Kliniken bzw. Ärzte vor einem HIV-Test die **Einwilligung der Patienten** dazu ein. In manchen Kliniken erteilt der Patient bereits im **Aufnahmevertrag** seine Einwilligung für den Fall, daß ein HIV-Test aus ärztlicher Sicht geboten ist. Datenschutzrechtliche Probleme sind in diesem Zusammenhang bei den Datenschutzkontrollen in Krankenhäusern bisher nicht bekannt geworden.

2.8 Alarmierung von Rettungsdienst und Notarzt über Rufnummer 112

Nach einem Antrag von Abgeordneten des Bayerischen Landtags soll die Staatsregierung prüfen, inwieweit die Einführung einer **bayernweiten gemeinsamen Rufnummer 112** für Rettungsdienst und Feuerwehr möglich ist.

In der Beratung dieses Antrags im Rechts- und Verfassungsausschuß des Landtags habe ich auf eine Datenschutzfrage hingewiesen, die mit der Rufnummer 112 verbunden ist:

Über den Notruf 112 wird derzeit primär die Feuerwehr alarmiert. Aber auch der **Rettungsdienst und der Notarzt** können über Notruf 112 angefordert werden. Der Notruf 112 geht jedoch in manchen Teilen Bayerns derzeit noch bei **Polizeidienststellen** ein. Wenn wegen einer Verletzung oder akuten Erkrankung über Nummer 112 ärztliche Hilfe angefordert wird, erfährt mit der Alarmierung des Rettungsdienstes/Notarztes **gleichzeitig die Polizei** den Vorfall und wird nach den gesetzlichen Bestimmungen (StPO, PAG) tätig. Die Organisation des Notrufs macht es den Bürgern praktisch unmöglich, sich **über die Notrufnummer 112 vertraulich an den Rettungsdienst oder den Notarzt zu wenden.**

Diese datenschutzrechtlichen Bedenken können nicht mit dem Hinweis ausgeräumt werden, daß für Rettungsdienst und Notarzt in Bayern auch der landeseinheitliche Notruf 19222 zur Verfügung steht, der bei den ständig besetzten Rettungsleitstellen eingeht. Da diese Nummer weniger bekannt ist, werden Rettungsdienst und Notarzt auch über Rufnummer 112 alarmiert.

Damit bei Unglücksfällen und sonstigen Notfällen der Rettungsdienst einschließlich des Notarztes ohne Angst vor strafrechtlicher Verfolgung alarmiert werden kann, müßte der Notruf 112 so geschaltet werden, **daß der Anruf nicht „bei der Polizei" eingeht.**

Der Ausschuß hat die Staatsregierung gebeten, auch zu der von mir vorgetragenen Problematik und zu Möglichkeiten der Verbesserung des Datenschutzes Stellung zu nehmen.

3. Sozialbehörden

3.1 Bürgereingaben

Im Berichtsjahr wandten sich wieder Bürger wegen Verletzungen des **Sozialgeheimnisses** an mich. Die meisten Petenten befürchteten, Sozialbehörden hätten ihre personenbezogenen Daten unzulässigerweise an andere Stellen übermittelt.

Ein Schwerpunkt der Eingaben war dabei die vermutete unzulässige Offenbarung gegenüber dem **Arbeitgeber**. In einigen Fällen waren die Beschwerden berechtigt, da die Sozialbehörden ohne Einschaltung des Petenten Sozialdaten an den Arbeitgeber offenbart hatten.

3.2 Umsetzung des Urteils des Bundesverfassungsgerichts zum Schwangerschaftsabbruch

Das Bundesverfassungsgericht hat mit Urteil vom 28. Mai 1993 § 218 a Abs. 1 und § 219 Strafgesetzbuch in der Fassung des Schwangeren- und Familienhilfegesetzes vom 27. Juli 1992 für nichtig erklärt. Damit ist die reine Fristenlösung, die einen von einem Arzt vorgenommenen Schwangerschaftsabbruch in den ersten 12 Wochen der Schwangerschaft nach Beratung für rechtmäßig erklärte, nichtig. Nach der **Anordnung des Bundesverfassungsgerichts** ist der Schwangerschaftsabbruch künftig nicht strafbar, wenn die Schwangerschaft innerhalb von 12 Wochen nach der Empfängnis durch einen Arzt abgebrochen wird, die schwangere Frau den Abbruch verlangt und dem Arzt durch eine **Bescheinigung** nachgewiesen hat, daß sie sich mindestens drei Tage vor dem Eingriff von einer anerkannten Beratungsstelle **hat beraten lassen.**

An die Beratung hat das Bundesverfassungsgericht präzise Anforderungen gestellt. So kann die schwangere Frau u.a. auf ihren Wunsch gegenüber der sie beratenden Person **anonym** bleiben. Sieht die beratende Person die Beratung als abgeschlossen an, so hat die Beratungsstelle der Frau auf Antrag über die Tatsache, daß eine Beratung stattgefunden hat, eine auf ihren Namen lautende und mit dem Datum des letzten Beratungsgesprächs versehene Bescheinigung auszustellen. Zur **Sicherstellung einer anonymen Beratung** gemäß der Anordnung des Bundesverfassungsgerichts halte ich folgende Vorkehrungen für erforderlich:

1. In den Beratungsstellen ist bei der Anmeldung mündlich und auch durch Aushang auf die Möglichkeit einer anonymen Beratung **hinzuweisen.**
2. **Protokolle** über anonyme Beratungen sind von den Durchschlägen der **Beratungsbestätigungen,** die den Namen der Beratenen enthalten, strikt zu trennen. Dies gilt sowohl für die **räumliche** Aufbewahrung als auch in **personeller** Hinsicht für die Verwaltung bzw. den Zugriff auf die Unterlagen. Auch inhaltlich darf keine Verbindung zwischen dem Protokoll einer bestimmten Beratung und den Bestätigungsdurchschlägen herstellbar sein.

3. Die **Beraterin** selbst kann im Fall einer anonymen Beratung die **Bestätigung** nicht unterzeichnen. Die Bestätigung muß deshalb von einer anderen Mitarbeiterin ausgestellt werden. Die Aufbewahrung eines Durchschlags der Beratungsbestätigung mit dem Namen der Beratenen einschließlich Geburtsdatum und Adresse wird aus Nachweisgründen und für den Fall, daß das Original verloren geht, akzeptiert.

   Das Arbeitsministerium hat deutlich herausgestellt, daß die Aufbewahrung einer Durchschrift allein dem **Schutz der Frau** dient: Bei Verlust oder Zerstörung durch Dritte vor Aufsuchen des Arztes könne ohne Probleme eine Zweitschrift ausgestellt werden. Nur so könne auch bei einem Verlust des Originals bei späteren Rechtsstreitigkeiten nachgewiesen werden, daß die Frau die Voraussetzungen für einen straffreien Abbruch erfüllt hat. Sollten Frauen jedoch wünschen, daß in der Beratungsstelle keine Kopie aufgehoben wird, werde auch diese Durchschrift ausgehändigt. Die Verweigerung der Aufbewahrung einer Durchschrift habe auf die Ausstellung der Beratungsbescheinigung keinen Einfluß.

4. Für die Aufbewahrung von Protokollen und Durchschlägen der Beratungsbestätigungen sollten **Fristen** festgelegt werden. Die Protokolle sollten vernichtet werden, sobald sie für Kontrollzwecke, insbesondere im Zusammenhang mit einer Wiedererteilung der Anerkennung der Beratungsstelle oder für wissenschaftliche Zwecke oder zur Überprüfung des Verfahrens nicht mehr benötigt werden. Solange noch keine gesetzliche Regelung getroffen ist, wird eine fünfjährige Aufbewahrung wie bei den bisherigen Bestätigungen nach dem bayerischen Schwangerenberatungsgesetz nicht beanstandet.

Die Anonymität des Verfahrens werde ich zu gegebener Zeit durch Kontrollen vor Ort überprüfen.

3.3 Verwendung von Versichertendaten durch Krankenkassen im Wettbewerb um Mitglieder für Werbezwecke

Im Berichtszeitraum hatte ich die Frage zu klären, ob eine gesetzliche Krankenkasse die Adressen ihrer Mitglieder nutzen darf, um diese im Zusammenhang mit **Neugründungen von Betriebskrankenkassen** anzuschreiben. Unter Berücksichtigung der Äußerung des Staatsministeriums für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit habe ich die Verwendung der Anschriften für zulässig erachtet, soweit sich die Aufklärung **im Rahmen einer sachlichen Information** bewegt und **nicht den Charakter einer gegen wettbewerbsrechtliche Grundsätze verstoßenden Werbung für eigene Zwecke** annimmt.

Nach § 284 Abs. 3 SGB V ist der Krankenkasse die Verwendung personenbezogener Daten auch für andere als in § 284 Abs. 1 genannte Zwecke gestattet, soweit dies durch Rechtsvorschriften des Sozialgesetzbuches angeordnet oder erlaubt ist. Eine solche Erlaubnis stellt § 13 SGB I dar. Die Vorschrift enthält eine Verpflichtung der Leistungsträger, im Rahmen ihrer Zuständigkeit „die Bevölkerung" über die Rechte und Pflichten nach dem Gesetzbuch aufzuklären. Die Aufklärung braucht sich aber nicht an Personen zu richten, die solche Rechte und Pflichten nicht haben können. Die Kassen haben damit die Möglichkeit, nur diejenigen zu unterrichten, die als Träger der betreffenden Rechte und Pflichten in Frage kommen.

Bei der Neugründung oder Erstreckung einer Betriebskrankenkasse entstehen solche Rechte und Pflichten für die beim betreffenden Arbeitgeber beschäftigten Kassenmitglieder, nicht aber für andere Teile der Bevölkerung. Pflicht der Krankenkasse nach § 13 SGB I ist daher eine sachliche Information **dieses Personenkreises.** Wenn die Krankenkassen aber zur Unterrichtung **der betroffenen** Mitglieder **verpflichtet** sind, dann umfaßt dieses Gebot auch die Befugnis zur Nutzung der Anschriften.

Die Verwendung der Anschriften zum Anschreiben der Mitglieder halte ich aber auch zur „Feststellung des Versicherungsverhältnisses und der Mitgliedschaft" nach § 284 Abs. 1 Nr. 1 SGB V für zulässig. Dies umfaßt notwendigerweise auch die angemessene Korrespondenz im Hinblick auf eine evtl. **Beendigung der Mitgliedschaft.** Ich halte es für notwendig, daß die Krankenkasse ihren Mitgliedern auf ihren Fall abgestellte objektive Informationen zukommen läßt, wenn eine Beendigung der Mitgliedschaft heransteht, und sie hierzu die Anschriften derjenigen Mitglieder nutzt, für die eine Beendigung der Mitgliedschaft in Frage kommt. Dies gilt jedenfalls von dem Zeitpunkt an, in dem die Errichtung oder Erstreckung der Betriebskrankenkasse nach den §§ 148, 149 SGB V genehmigt ist, weil dann die Mitglieder über die Fortführung ihrer Mitgliedschaft bei der bisherigen gesetzlichen Krankenkasse entscheiden müssen.

3.4 Frage nach der Erwerbstätigkeit einer Pflegeperson

In einer Eingabe wurde bemängelt, daß im Fragebogen einer Krankenkasse zum Antrag auf Pflegegeld auch detaillierte **Auskünfte über Pflegepersonen** verlangt werden. So werde beispielsweise neben den Personalien der Pflegeperson auch deren **Erwerbstätigkeit** abgefragt. Erfahrungsgemäß würden jedoch manche Helfer die Tätigkeit als Pflegeperson aufgeben, wenn über sie Auskünfte erteilt werden müßten.

Bei der schwerpunktmäßigen Prüfung von Ortskrankenkassen im Vorjahr war Gegenstand der Kontrolle auch die Erhebung personenbezogener Daten durch Formulare. Bei der Prüfung des in Frage stehenden Formulars „Antrag auf Pflegegeld" habe ich festgestellt, daß es keine der geprüften Krankenkassen für erforderlich hielt, auch **die Art der Erwerbstätigkeit der Pflegepersonen** abzufragen. Während zwei Krankenkassen die Frage im Formular überhaupt nicht aufgenommen hatten, erklärten sich zwei andere Ortskrankenkassen bereit, diese

Frage in den Formularen künftig nicht mehr zu stellen, weil sie für die Anerkennung einer Pflegeperson ohne Bedeutung ist. Nach § 57 Abs. 2 SGB V dürfen Geldleistungen nach Abs. 1 zwar nur dann gezahlt werden, wenn die Pflegeperson auch bei Ausübung einer Erwerbstätigkeit zu einer ausreichenden Pflege in der Lage ist. Ausschlaggebend dabei ist jedoch, ob die Pflegeperson trotz ihrer sonstigen Inanspruchnahme (wöchentliche Arbeitszeit) **noch genügend Zeit für eine ausreichende Pflege** hat. Entscheidend für die Beurteilung dieser Frage ist nach meinen Feststellungen bei den Kontrollen der Krankenkassen also die **wöchentliche Arbeitszeit,** nach der somit gefragt werden darf, nicht jedoch die Art der sonstigen Erwerbstätigkeit der Pflegeperson.

Der Landesverband der Ortskrankenkassen hat sich meiner Auffassung zwischenzeitlich angeschlossen und die Krankenkassen in diesem Sinne informiert.

3.5 Angabe von Heilstätten bei Kurbewilligungen gegenüber Arbeitgebern

Im Berichtszeitraum wurde ich darauf aufmerksam gemacht, daß Arbeitnehmer, denen eine Kur bewilligt wurde, den exakten Beginn der Kur dem Arbeitgeber **unter Vorlage des Einberufungsschreibens der Behandlungsstätte** mitteilen müssen. Es bestehe daher die Gefahr, daß Personalsachbearbeiter anhand der genannten **Behandlungsstätte** auch auf die **Art der zu behandelnden Erkrankung** schließen können. Problematisch kann die Offenbarung der Behandlungsstätte gegenüber dem Arbeitgeber insbesondere dann sein, wenn bekannt ist, daß sich die Einrichtung auf die Nachbehandlung bestimmter sensibler Krankheitsbilder, wie z.B. Suchtprobleme oder psychische Erkrankungen, spezialisiert hat.

Nach § 7 Abs. 2 Lohnfortzahlungsgesetz ist der Arbeitnehmer verpflichtet, dem Arbeitgeber unverzüglich eine **Bescheinigung über die Bewilligung** der Kur vorzulegen und den Zeitpunkt des Kurantritts **mitzuteilen.** Dieser Wortlaut verpflichtet den Arbeitnehmer jedoch nicht, auch eine **Bescheinigung der Behandlungsstätte** über den Zeitpunkt des Kurantritts vorzulegen. Ein bayerischer Rentenversicherungsträger teilte auf Rückfrage mit, daß eine **formlose Mitteilung des Arbeitnehmers** an den Arbeitgeber genügen müßte. Sollte der Arbeitgeber – was nur in Ausnahmefällen vorkommen dürfte – Zweifel an der Richtigkeit der Aussage über den Kurantritt haben, könnte er sich erforderlichenfalls an den Kostenträger wenden.

Diese Verfahrensweise begrüße ich aus datenschutzrechtlicher Sicht, da dem Versicherten freigestellt wird, ob er dem Arbeitgeber das Einberufungsschreiben der Behandlungsstätte oder lediglich eine formlose Mitteilung des Kurantritts übergibt. Der Versicherte sollte **schriftlich** auf diese Wahlmöglichkeit hingewiesen werden. Ein solcher Passus könnte z.B. in die Hinweise des Kurbewilligungsbescheides aufgenommen werden. Der Rentenversicherungsträger hat mir zugesichert, die Versicherten schriftlich auf die Möglichkeit einer neutralen Bescheinigung hinzuweisen.

3.6 Sozialdatenschutz im gerichtlichen Verfahren (Sammelklagen)

Von einem anderen Landesdatenschutzbeauftragten wurde die Frage aufgeworfen, ob eine gesetzliche Krankenkasse in einem sozialgerichtlichen Verfahren mittels **einer** Klageschrift auf Feststellung der Unwirksamkeit des Beitritts von 31 Beschäftigten zu einer Ersatzkasse (der Beklagten) klagen darf oder **31 gesonderte Klagen** erheben muß. Die datenschutzrechtliche Problematik liegt darin, daß die Versicherten voraussichtlich gemäß § 75 Sozialgerichtsgesetz (SGG) **beigeladen** und damit Beteiligte des Rechtsstreites werden (§ 69 SGG). Ihnen ist die Klageschrift und der weitere Schriftverkehr zuzusenden, so daß Sozialdaten der einzelnen Versicherten auch den anderen bekannt werden.

Das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit teilte dazu mit, daß die Problematik von **Sammelklagen** bei den bayerischen Sozialgerichten nicht in der geschilderten Intensität aufgetreten sei. Soweit Sammelklagen bei den Sozialgerichten anhängig gewesen seien, hätten die Kammervorsitzenden auch unter Berücksichtigung der datenschutzrechtlichen Fragen überwiegend eine **Trennung** der anhängigen Rechtsstreitigkeiten **nicht** für erforderlich gehalten.

In Übereinstimmung mit dem Präsidenten des Bayerischen Landessozialgerichts sei jedoch die Auffassung zu vertreten, daß der verfassungsrechtlich gebotene Schutz der Persönlichkeit eine **verfassungskonform einschränkende Auslegung** des § 120 SGG erfordere. Das Gericht, dem Sozialdaten offenbart worden seien, sei nach § 78 SGB X verpflichtet, die übermittelten Daten nur zweckentsprechend zu verwenden und im übrigen das Sozialgeheimnis zu wahren. Zur Erfüllung dieser Verpflichtung könne sich das Gericht der Instrumentarien des Verfahrensrechts bedienen, d.h. im konkreten Fall Verfahren **trennen** bzw. verbinden oder den Verfahrensbeteiligten aufgeben, Stellungnahmen **einzelfallbezogen** oder bezüglich der nichtbetroffenen Beteiligten **geschwärzt** vorzulegen, aber auch die **Akteneinsicht** aus datenschutzrechtlichen Gründen **untersagen.**

Diese Auffassung begrüße ich. Wie ich bereits im 14. Tätigkeitsbericht zur Gewährung von Akteneinsicht im staatsanwaltschaftlichen Ermittlungsverfahren ausgeführt habe, sollte auch im sozialgerichtlichen Verfahren bei der Entscheidung über die Akteneinsicht **abgewogen** werden zwischen dem Interesse des Antragstellers und dem Persönlichkeitsrecht der Betroffenen (14. Tätigkeitsbericht, 6.10.1, S. 52).

Darüber hinaus ist der Auffassung des Arbeitsministeriums zuzustimmen, daß die **Sozialleistungsträger** im Falle der Klageerhebung und bei der Abgabe von Stellungnahmen, soweit sie sich auf eine Vielzahl von Betei-

ligten eines Rechtsstreits beziehen, für die Notwendigkeit des Sozialdatenschutzes **zu sensibilisieren sind.**

3.7 Offenbarungsbefugnis von Sozialbehörden bei Verdacht von Kindesmißhandlungen

Bereits im 14. Tätigkeitsbericht hatte ich mich mit der Frage auseinanderzusetzen, ob ein Mitarbeiter eines Jugendamtes bei Verdacht der Kindesmißhandlung eine Offenbarungsbefugnis gegenüber Strafverfolgungsbehörden hat. Im Berichtszeitraum hatte ich mich mit einer vergleichbaren Situation zu befassen. Es stellte sich die Frage, ob eine Mitarbeiterin im Sachbereich **Beratungsstelle** einem Aufenthaltsbestimmungspfleger derselben Sozialbehörde im Sachgebiet **Erziehungshilfe** personenbezogene Daten offenbaren darf, damit dieser prüfen könne, ob das Umgangsrecht des Vaters mit seinen Kindern auf Grund des Verdachts des sexuellen Mißbrauchs eingeschränkt werden müsse.

Im Vordergrund steht die Frage, ob es sich bei den Daten, welche die Beratungsstelle an die Erziehungshilfe übermitteln soll, um solche Daten handelt, die ihr zum Zweck persönlicher und erzieherischer Hilfe **anvertraut** worden sind. Nach § 65 SGB VIII dürfen solche personenbezogenen Daten nur unter eng begrenzten Voraussetzungen offenbart werden. Dabei genügt jedoch das Einweihen in eine persönliche Angelegenheit für sich alleine nicht, um Vertraulichkeit herzustellen. Es ist immer erforderlich, daß der **Zweck persönlicher und erzieherischer Hilfe** verfolgt wird.

Davon abgesehen ist auch beim Anvertrauen von Daten nach § 65 SGB VIII eine Offenbarung gegenüber Dritten nicht generell ausgeschlossen. Vielmehr ist die Offenbarung unter engen Voraussetzungen zulässig, wobei im konkreten Fall die Möglichkeit des rechtfertigenden Notstands nach § 34 StGB in Frage kommt. Voraussetzung hierfür ist eine **gegenwärtige, nicht anders abwehrbare Gefahr für Leib und Leben.** Wenn die Mitarbeiterin der Beratungsstelle feststellt, daß sich nach den Angaben der Kinder der Verdacht des sexuellen Mißbrauchs bestätigt, besteht der begründete Verdacht, daß weitere Besuche beim Vater eine Gefahr für Leib und Leben der Kinder darstellen. In diesem Falle wäre eine gegenwärtige Gefahr zu bejahen und die Offenbarung der Daten an das Sachgebiet Erziehungshilfe zulässig und möglicherweise auch **dringend geboten.**

Falls eine gegenwärtige Gefahr nicht zu bejahen ist, kann nach herrschender Meinung eine Offenbarung zulässig sein zur **Wahrung entgegenstehender berechtigter allgemeiner oder fremder Interessen,** soweit die Offenbarung unter Berücksichtigung der widerstreitenden Interessen ein angemessenes Mittel dazu ist. Die Mitarbeiterin der Beratungsstelle hat eine sorgfältige Abwägung vorzunehmen. Falls weitere Mißhandlungen der Kindern zu befürchten sind, dürfte die Information an den Aufenthaltbestimmungspfleger den Kindesinteressen am ehesten entsprechen, um den Umgang des Vaters mit den Kindern zu beschränken.

4. Polizei

4.1 Zur Lage des Datenschutzes

4.1.1 Negative Auswirkungen des neuen Bayerischen Datenschutzgesetzes

Das Berichtsjahr 1993 brachte für die **Datenschutzkontrolle und damit unmittelbar für den Datenschutz der Bürger** bei der polizeilichen Datenverarbeitung einen deutlichen Rückschlag.

Das ab 1. März 1994 geltende neue Bayerische Datenschutzgesetz schränkt die **Kontrollbefugnisse des Landesbeauftragten** für den Datenschutz und damit den **Datenschutz aller Bürger** im Vergleich zu dem in Deutschland inzwischen erreichten Standard massiv ein: Durch den **Aufschub der Erhebungskontrolle** bis zum Abschluß des Strafverfahrens und durch die **bloße Anlaßkontrolle bei Datenverarbeitung in Akten** wird die vom Bundesverfassungsgericht geforderte unabhängige externe Datenschutzkontrolle gerade bei der Polizei **nachhaltig und völlig grundlos behindert.**

4.1.1.1 Aufschub der Erhebungskontrolle

Durch die **Sondervorschrift** des Art. 30 Abs. 4 Satz 1 BayDSG wird die Kontrolle des Landesbeauftragten über die **Erhebung** von Daten, welche Polizei und Staatsanwaltschaft in strafrechtlichen Ermittlungsverfahren durchführen, zwar nicht ausgeschlossen, aber bis zum Abschluß des Strafverfahrens **aufgeschoben.** Diese Regelung ist einmalig in der Bundesrepublik. Sie verhindert eine zeitnahe externe Kontrolle der Datenerhebung durch den Landesbeauftragten für den Datenschutz. Ein Aufschub der Datenschutzkontrolle bis zum Abschluß des Strafverfahrens ist vor allem in folgenden Fällen **unvertretbar:**

a) bei **tiefergehenden Eingriffen** in das informationelle Selbstbestimmungsrecht – beispielsweise längerfristige Observation, verdeckter Einsatz von technischen Mitteln wie Foto- und Videogeräten, Peilsendern, Bewegungsmeldern (§ 100 c Abs. 1 Nr. 1 StPO), Einsätze verdeckter Ermittler, die sich nicht gegen einen bestimmten Beschuldigten richten und außerhalb von Wohnungen durchgeführt werden (§ 110 b Abs. 1 StPO).
   Diese Maßnahmen
   - werden **ohne Wissen** des Betroffenen durchgeführt,
   - sind nicht nur gegen Beschuldigte oder Verdächtige, sondern auch gegen andere **völlig unverdächtige Personen** gerichtet, z. B. Angehörige, Freunde, Bekannte, Geschäftsfreunde, Kunden, nach Maßgabe der §§ 100 c Abs. 2, 110 b Abs. 1 StPO und
   - bedürfen keiner richterlichen Anordnung oder Bestätigung.

b) bei **langdauernden Strafverfahren,** in denen die Kontrolle durch die Sondervorschrift zeitlich weit hinausgeschoben wird, oder

c) wenn gegen den Betroffenen überhaupt kein Strafverfahren anhängig ist.

Besonders problematisch ist der Aufschub der Datenschutzkontrolle, wenn eine **Vielzahl Unverdächtiger** von den Ermittlungsmaßnahmen betroffen werden. Diese Personen haben keine Möglichkeit, sich gegen unzulässige Fahndungsmaßnahmen zu wehren, da sie regelmäßig keine Kenntnis von der Datenerhebung und anschließenden Speicherung und Nutzung haben. In diesen Fällen ist eine uneingeschränkte Kontrollmöglichkeit – wie in allen anderen Bundesländern – zum Schutz des informationellen Selbstbestimmungsrechts unverzichtbar.

4.1.1.2 Bloße Anlaßkontrolle bei Datenverarbeitung in Akten

Die zweite Einschränkung meiner Kontrollbefugnisse betrifft die gesamte Datenerhebung und -verarbeitung in Akten. Durch die **Sondervorschrift** des Art. 30 Abs. 1 Satz 2 BayDSG wird meine Kontrolle über die Erhebung und Verarbeitung von Daten in und aus Akten auf eine **bloße Anlaßkontrolle** beschränkt. Diese Beschränkung hat zur Folge, daß ein **erheblicher Teil der Erhebung und Verarbeitung** von personenbezogenen Daten durch die Polizei **gegenüber der externen Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz mehr oder weniger abgeschottet** ist. Dadurch wird die Datenschutzkontrolle insbesondere in denjenigen Bereichen massiv erschwert, in denen die Bürger wegen **verdeckter Tätigkeit der Polizei** in besonderer Weise des Schutzes einer unabhängigen Institution bedürfen. Der Landesbeauftragte erhält im **besonders sensiblen Bereich** verdeckter Informationsbeschaffung und -verarbeitung **nur sporadisch Einblick** in die Erhebung und Verarbeitung von Daten in Akten. Denn der Bürger weiß von den verdeckten Maßnahmen nichts und kann sich deshalb nicht an mich wenden. Der Landesbeauftragte wiederum erfährt ebenfalls – von Zufallsfunden bei Dateikontrollen abgesehen – keine Anhaltspunkte und kann deshalb nicht tätig werden. Fehler und Mißbräuche werden dem Landesbeauftragten für den Datenschutz im wesentlichen nur bekannt, soweit sie ausnahmsweise einem betroffenen Bürger auffallen, der sich dann beschwert oder die Presse unterrichtet, oder wenn der Landesbeauftragte durch Zufall bei einer Dateikontrolle darauf stößt. Für den Datenschutz der Bürger bedeutet die bloße Anlaßkontrolle im Bereich der verdeckten Ermittlungen eine Beeinträchtigung, die durch nichts gerechtfertigt ist.

4.1.2 Elektronische Beweissicherung in Gangsterwohnungen („Großer Lauschangriff")

Eine allerdings schrumpfende Mehrheit der Datenschutzbeauftragten des Bundes und der Länder spricht sich bisher noch gegen eine Grundgesetzänderung zur Zulassung des verdeckten Abhörens und Herstellens von Bild- und Tonaufzeichnungen in und aus Gangsterwohnungen für Zwecke der Strafverfolgung aus und hält eine solche Maßnahme allenfalls in Hotelzimmern, Garagen u. ä. für denkbar.

Die Ablehnung der elektronischen Beweissicherung für das Strafverfahren unter Hinweis auf die Menschenwürde ist umso unverständlicher, als bereits derzeit nach geltendem Verfassungsrecht der Einsatz solcher Raumüberwachungsmittel in Wohnungen zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung zulässig ist. Das heißt:

Zur Verhinderung von Rauschgifthandel dürfen Verhandlungen in Gangsterwohnungen schon heute mit Wanzen abgehört werden. Dann kann doch das künftige Abhören zur Strafverfolgung und zum Außerverkehrziehen von Gangstern nicht gegen die Menschenwürde verstoßen. Oder verstößt gar bereits unsere geltende Verfassung gegen die Menschenwürde, weil sie den" Großen Lauschangriff" zur Gefahrenabwehr bereits zuläßt? Daraus wird deutlich, wie abgründig die Auffassung der Mehrheit der Datenschützer ist. Im übrigen zeigt allein schon die Verwendung des Begriffs „Großer Lauschangriff", daß ein Teil der deutschen Gesellschaft noch nicht einmal begriffen hat, daß ihre Freiheit nicht vom demokratischen Rechtsstaat, sondern vom organisierten Verbrechen bedroht ist.

Ich habe den Einsatz solcher Mittel in Wohnungen (auch in Privatwohnungen) unter strengen Voraussetzungen stets befürwortet, weil ich diesen Einsatz zur Bekämpfung schwerster Verbrechen der organisierten Kriminalität nach den unbestreitbaren Erfahrungen der Polizei für inzwischen unabdingbar notwendig halte. Westeuropa und Deutschland sind einem zielgerichteten Angriff internationaler organisierter Kriminalität ausgesetzt. Die offene Gesellschaft in Deutschland darf aber nicht zum wehrlosen Spielball der internationalen Mafia werden. Es geht dabei weniger um die Aufklärung des einen oder anderen Verbrechens als vielmehr um die **Abwehr einer unmittelbar bevorstehenden Gefahr für die Existenz unserer freiheitlichen humanen Gesellschaftsordnung.** Leben und Freiheit, die durch die internationale organisierte Kriminalität bedroht sind, sind höher einzuschätzen als Gangsterwohnungen, in denen konspirative Gespräche von Schwerstkriminellen abgehört werden. Die **Menschenwürde** wird durch das Abhören von Gangsterwohnungen nicht verletzt. Bei der Frage, was Menschenwürde beinhaltet, ist vom **Menschenbild des Grundgesetzes** auszugehen. Hierzu sei an die Rechtsprechung des Bundesverfassungsgerichts erinnert: Das Grundgesetz ist eine wertgebundene Ordnung, die den Schutz von Freiheit und Menschenwürde als obersten Zweck allen Rechts erkennt; sein Menschenbild ist **nicht das des selbstherrlichen Individuums**, sondern das **der in der Gemeinschaft stehenden und ihr vielfältig verpflichteten Persönlichkeit** (BVerfGE 12, 51). Angesichts der Größe der Gefahr, die vom organisierten Verbrechen für unsere humane Gesellschaft und für Freiheit und Würde des Einzelnen ausgeht, erscheint mir das Abhören von Gesprächen in Gangsterwohnungen, selbst

wenn dabei auch Dritte betroffen werden, unter strengen Voraussetzungen angemessen, vertretbar und zumutbar.

In meinem 14. Tätigkeitsbericht habe ich zur Zulässigkeit einer Grundgesetzänderung ausgeführt:

> „Die Gestattung des Einsatzes von Observationsmitteln in Wohnungen ist **die durch die Not erzwungene Fortentwicklung des Verfassungsrechts.** Es ist vorrangige Aufgabe des Rechtsstaats, das weitere Eindringen der organisierten Kriminalität in die Gesellschaft zu verhindern. Eine Gesellschaft, die unfähig ist, ihre Bürger vor diesem Übel zu schützen, verliert ihre Existenzberechtigung.
>
> Ein Blick über die deutschen Grenzen könnte auch hier sehr hilfreich sein. Wenn in fast allen westlichen Staaten mit ungebrochener rechtsstaatlicher Tradition der Einsatz von Observierungsmitteln in Wohnungen gegen Schwerstverbrecher der organisierten Kriminalität nicht gegen die Menschenwürde verstößt und erfolgreich praktiziert wird, dann kann auch in Deutschland die Menschenwürde nicht verletzt sein."

Entgegen der Auffassung des Bundesbeauftragten für den Datenschutz ist der Verfassungsgeber des Grundgesetzes durch die Wesensgehaltsschranke des Art. 19 Abs. 2 Grundgesetz nicht daran gehindert, elektronische Observationsmittel in Wohnungen zuzulassen. Die Wesensgehaltsschranke gilt nicht für den Verfassungsgeber. Das Grundrecht auf Unantastbarkeit der Wohnung (Art. 13 GG) ist schon bisher im Grundgesetz nur eingeschränkt garantiert und kann durch das Grundgesetz unter Beachtung des Grundsatzes der Verhältnismäßigkeit weiter eingeschränkt werden.

Der Einsatz von elektronischen Raumüberwachungsmitteln darf nur unter **strengen Voraussetzungen** zugelassen werden:

1. Festlegung **enger materiell-rechtlicher Voraussetzungen** im Grundgesetz und insbesondere in der Strafprozeßordnung (StPO): beispielsweise Einsatz als ultima ratio zur Aufklärung von Mord und ähnlich schweren Verbrechen sowie schwerster Verbrechen der organisierten Kriminalität wie Rauschgift-, Kriegswaffen- und Menschenhandel, die in einem geschlossenen Straftatenkatalog aufgeführt werden
2. **Verwertungsverbot** von Erkenntnissen für die Verfolgung geringerer Straftaten, unverzügliche Vernichtung von Erkenntnissen über unbeteiligte Dritte
3. Genehmigung des Einsatzes im Einzelfall durch einen Senat des **Oberlandesgerichts**
4. Zusätzliche Genehmigung des Antrags der Staatsanwaltschaft auf Zulassung des Einsatzes durch den **Innen- oder Justizminister (persönliche Ministerverantwortung)**
5. **Jährlicher ausführlicher** Bericht des Ministers an das Parlament mit öffentlicher Aussprache, ähnlich der Praxis in den USA (über Betroffene, Wirksamkeit, Kosten etc.), soweit nicht zwingende Gründe der Geheimhaltung entgegenstehen **(Transparenz)**
6. **Unterrichtung** des Betroffenen so bald wie möglich (Eröffnung des Rechtswegs)
7. Jederzeitige uneingeschränkte Kontrolle durch die jeweiligen **Datenschutzbeauftragten** über die Verarbeitung und Verwendung der Daten

Die vorherige Genehmigung des Einsatzes durch einen Parlamentsausschuß halte ich für systemfremd und nicht sachgerecht, da die vorausgehende Befassung des Parlaments, das den Einsatz billigt, die nachträgliche wirksame Kontrolle erheblich erschweren könnte.

Mehr Transparenz und uneingeschränkte Datenschutzkontrolle

Im Zusammenhang mit der Zulassung des Einsatzes elektronischer Raumüberwachungsmittel sollten zur besseren Gewährleistung des Persönlichkeitsschutzes beim Eindringen der Justiz in die Privatsphäre für derzeit bereits zulässige Maßnahmen folgende **zusätzlichen Sicherungsvorkehrungen** getroffen werden:

1. Einbeziehung der Telefonabhöraktionen (§ 100 a StPO) in die **Berichtspflicht gegenüber dem Parlament** (wie künftig bei elektronischer Raumüberwachung) sowie **Unterrichtung der Datenschutzbeauftragten** über genehmigte bzw. durchgeführte Abhöraktionen und umfassende Kontrollkompetenzen dieser Stellen. **Die gerichtliche Genehmigung der Maßnahme gewährleistet noch keinen datenschutzgerechten Umgang mit den gewonnenen Erkenntnissen.**
2. **Uneingeschränkte Datenschutzkontrolle durch die Datenschutzbeauftragten des Bundes** und **aller** Länder, insbesondere auch über Maßnahmen der Staatsanwaltschaft, der Polizei und des Verfassungsschutzes (im Bund sowie in den Ländern Baden-Württemberg, Bayern und Sachsen-Anhalt besitzen die Datenschutzbeauftragten bei der Datenverarbeitung in/aus Akten eine Kontrollbefugnis nur bei konkretem Anlaß, z. B. bei Beschwerden – **sogenannte Anlaßkontrolle.** Dies ist insbesondere im Bereich häufig verdeckter Ermittlungen durch Staatsanwaltschaft, Polizei und Verfassungsschutz im Hinblick auf einen ausreichenden Datenschutz völlig inakzeptabel). Es muß also gewährleistet werden, daß im Bund wie in allen Ländern bei der Datenverarbeitung in/aus Akten die Beschränkung der Datenschutzkontrolle auf eine Anlaßkontrolle ausgeschlossen ist.

4.1.3 Neue Richtlinien für polizeiliche Datensammlungen (PpS-Richtlinien)

Grundlage für die Führung kriminalpolizeilicher personenbezogener Sammlungen von Bürgerdaten zur Erfüllung der Aufgaben der Polizei auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr waren bisher verwal-

tungsinterne Richtlinien aus dem Jahre 1981. Bereits in meinen 13. Tätigkeitsbericht hatte ich vom Innenministerium gefordert, die Richtlinien und Dienstanweisungen für die polizeiliche Datenverarbeitung an das Polizeiaufgabengesetz vom 1. Oktober 1990 anzupassen. Im 14. Tätigkeitsbericht habe ich darauf hingewiesen, daß der Überprüfung u.a. auch die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) bedürfen. Nunmehr hat das Innenministerium den Entwurf der neugefaßten Richtlinien vorgelegt, die im Hinblick auf den Inhalt der Sammlungen, der nicht allein auf **kriminalpolizeiliche** Unterlagen beschränkt ist, in Richtlinien für die Führung **polizeilicher** personenbezogener Sammlungen (PpS-Richtlinien) umbenannt wurden. In einem Gespräch mit dem Innenministerium konnte in einer Reihe von Punkten aus datenschutzrechtlicher Sicht eine Verbesserung des Entwurfs erreicht werden (im einzelnen unter Nr. 4.9).

4.1.4 Auflösung des Regional-Kriminalaktennachweises (R-KAN)

Im Zusammenhang mit der Einrichtung der Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung und Verbrechensbekämpfung (PSV)" auf der Grundlage eines integrierten polizeilichen Gesamtverfahrens **entfällt die bisherige Datei R-KAN** als selbständige Datei. An der **Kriminalaktenhaltung** der bayerischen Polizei ändert sich durch die Einrichtung der Datei PSV nichts: Vorgänge, die bisher für die Aufnahme in eine Kriminalakte bestimmt waren oder zur Anlage einer Kriminalakte geführt haben, sollen grundsätzlich auch weiterhin dort abgelegt werden. Allerdings erfolgt der Nachweis von Kriminalakten, die **ausschließlich** Unterlagen enthalten, die nicht in den Dateien Landes-/Bundes-KAN nachgewiesen werden dürfen, **künftig über die Datei PSV.** Die bisherigen Datenbestände des R-KAN sollen, sobald die technischen Voraussetzungen geschaffen sind, in die Dateien Landes-KAN bzw. PSV übertragen werden.

Gegen die Auflösung des R-KAN mit der Folge, daß ein Teil der Bestände in den Landes-KAN übernommen wird, bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken. Die Regionalisierung des Kriminalaktennachweises war eine bayerische Besonderheit, die aus Datenschutzgründen nicht geboten war. Darüber hinaus wird mit der Datei PSV eine regionale Speicherungsebene für Vorgänge geboten, die nicht KAN-relevant sind. Allerdings sind künftig im Bereich der Gefahrenabwehr Speicherungen im größeren Umfang als bisher für den landesweiten Abruf im KAN vorgesehen (z.B. Vermißte, Suizidversuche). Das Innenministerium hat diese landesweite Abrufbarkeit mit der Notwendigkeit einer effektiven Gefahrenabwehr nachvollziehbar begründet.

4.1.5 Integriertes Gesamtverfahren der Bayerischen Polizei (IGV-P)

Das Innenministerium ist dabei, ein EDV-Verfahren (IGV-P) für die Bayerische Polizei zu entwickeln, das es ermöglicht, personenbezogene Daten nach Erfassung in der Datei Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV) nach Bedarf automatisiert in andere Dateien (z.B. Kriminalaktennachweis) zu übertragen **(Grundsatz der Einmalerfassung).**

Durch die Einmalerfassung wird der Umfang der Zugriffsmöglichkeiten des einzelnen Polizeibeamten nicht erweitert. Ein übersichtliches System der **Zugriffsberechtigungen** nach **Ebenen** (Präsidium, Direktion, Inspektion, Dienstgruppe usw.) und nach **Funktionen** (Dienststellenleiter, Dienstgruppenleiter, Sachbearbeiter usw.) gewährleistet, daß der einzelne Polizeibeamte nur die Daten abrufen kann, die er zu seiner regelmäßigen Aufgabenerfüllung auch benötigt. Über die vergebenen Einzelberechtigungen sind von den Polizeipräsidien bzw. Polizeidirektionen aktuelle **Nachweise** zu führen.

Grundsätzliche datenschutzrechtliche Bedenken gegen das sog. Integrierte Gesamtverfahren habe ich nicht. Es erleichtert die polizeiliche Arbeit und trägt durch den Wegfall mehrfacher Erfassungsvorgänge zur Vermeidung von **Übertragungsfehlern** bei. Die Möglichkeit, durch automatisierte Verknüpfung personenbezogener Daten in den verschiedenen Dateien des Informationssystems der Bayerischen Polizei umfassende Persönlichkeitsprofile zu erstellen, wird **durch IGV-P nicht eröffnet.** Abfragen müssen wie bisher nach einzelnen Dateien **getrennt** erfolgen. Den Gefahren des **Datenmißbrauchs** kann mit ausreichenden **Zugriffsschutzverfahren** begegnet werden. Die vom Innenministerium dazu vorgesehenen Regelungen erscheinen mir nach vorläufiger Bewertung schlüssig und widerspruchsfrei. Eine abschließende Beurteilung wird erst nach Einsatz des Verfahrens im Echtbetrieb und seiner datenschutzrechtlichen Prüfung bei einer Polizeidienststelle möglich sein.

4.1.6 Abbau bürokratischer Vollzugshemmnisse

In einem Schreiben an die Datenschutzbeauftragten des Bundes und der Länder habe ich auf den besorgniserregenden Anstieg der Kriminalität und die gleichzeitige Abnahme der Aufklärungsquote hingewiesen. Auch wenn sich hieraus kein unmittelbarer Einfluß des Datenschutzes ableiten läßt, müssen sich die Datenschutzbeauftragten angesichts der sich rapide verschlechternden Lage der inneren Sicherheit fragen, ob die Arbeit der Polizei durch **zu strenge datenschutzrechtliche Anforderungen** behindert wird. Ich sehe derartige Behinderungen insbesondere in einer **übertriebenen Regelungsdichte datenschutzrechtlicher Vorschriften.** Dies führt dazu, daß die Polizei immer mehr gezwungen ist, die Straftaten „datenschutzgerecht zu verwalten" statt sie effektiv zu bekämpfen, und dadurch bei der Wahrnehmung ihrer wichtigsten Aufgaben der Verbrechensbekämpfung behindert wird. Ich bin deshalb der Auffassung, daß nicht nur bei der Forderung nach zusätzlichen Regelungen und Empfehlungen des Datenschutzes zu Gesetzgebungsvorhaben **Zurückhaltung** geboten ist, sondern daß die in

den letzten 15 Jahren erlassenen Gesetze **auf übertriebene Schutzvorschriften überprüft** werden sollten.

Die Polizei bleibt aufgefordert, diejenigen Datenschutzbestimmungen zu benennen, die einer wirksamen Verbrechensbekämpfung entgegenstehen. Sollte eine Abwägung zwischen der Sicherheit des Staates und seiner Bürger und dem Recht auf informationelle Selbstbestimmung im Einzelfall zu Ungunsten des Datenschutzes ausfallen, so muß Abhilfe möglich sein.

4.1.7 Erfolgskontrolle polizeilicher Befugnisse

Ein Datenschutzbeauftragter eines anderen Landes hat in diesem Zusammenhang vorgeschlagen, eine Erfolgskontrolle polizeilicher Befugnisse mit der **Tendenz zur Einschränkung bzw. Abschaffung von Befugnissen** durchzuführen. Zu diesem Zweck sollen alle Datenschutzbeauftragten in einem Schreiben an die für die innere Sicherheit im Bund und in den Ländern verantwortlichen Minister und Senatoren herantreten mit der Bitte, die Möglichkeiten zu benennen, um die Befugnisse und Instrumente der Strafverfolgung, Gefahrenabwehr und vorbeugenden Verbrechensbekämpfung auf ihre Geeignetheit und Wirksamkeit zu untersuchen sowie Stellung dazu zu nehmen, wie für vorhandene und künftige Regelungen sichergestellt werden könne, daß Unbeteiligte von den Maßnahmen zur Verbrechensbekämpfung so wenig wie möglich betroffen werden. Die Mehrheit der Datenschutzbeauftragten hat sich diesem Vorschlag angeschlossen.

Grundsätzlich ist eine Erfolgskontrolle polizeilicher Befugnisse und damit die Überprüfung, ob Eingriffsmöglichkeiten und die damit verbundenen Datenerhebungen erforderlich sind, zu begrüßen. Allerdings müßte für eine derartige Erfolgskontrolle ein konkreter Anlaß bestehen. Die Mehrheit der Datenschutzbeauftragten sieht einen solchen Anlaß im sprunghaften Anstieg der Kriminalität: **die polizeilichen Befugnisse hätten den Anstieg der Kriminalität nicht verhindern können, deshalb seien sie fragwürdig.** Diese Argumentation erscheint mir nun doch etwas naiv. Ein allgemein gehaltener Auftrag zur Überprüfung der Geeignetheit und Wirksamkeit polizeilicher Befugnisse führt erfahrungsgemäß nur zu einer ebenso allgemein gehaltenen Antwort, die die Notwendigkeit sämtlicher polizeilicher Befugnisse bestätigt. Soll eine derartige Anfrage bei der Polizei überhaupt sinnvoll sein, muß von seiten der Datenschutzbeauftragten aufgrund ihrer Prüfungserfahrungen konkret dargelegt werden, wo Zweifel an der Effizienz einzelner Maßnahmen bestehen. Der Umstand, daß von einer bestimmten Befugnis in einem bestimmten Zeitraum nicht oder nur wenig Gebrauch gemacht worden ist, läßt aber keinerlei Schlüsse zu, daß die Befugnis eingeschränkt oder abgeschafft werden müßte. Im übrigen dürfte der Anstieg der Kriminalität eher als Beleg dafür herangezogen werden, daß die polizeilichen Befugnisse noch nicht ausreichen. Aus diesen Gründen werde ich mich an dieser aufwendigen, zudem noch sinnlosen Aktion nicht beteiligen.

4.2 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren

- **allgemeine Kontrollen** von Dateien und Karteien, insbesondere von Dateien zur Gefahrenabwehr und Strafverfolgung (sog. GAST-Dateien), der Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung – Verbrechensbekämpfung (PSV)", der „Arbeitsdatei PIOS-Innere Sicherheit (APIS)", des „Kriminalaktennachweises (KAN)", der „Arbeitsdatei organisierte Kriminalität (ADOK)", des „Grenzaktennachweises (GAN)", des „Spurendokumentationssystems (SPUDOK)" und der Kartei „Psychisch Kranke – psychisch Gestörte"
- Prüfung des Entwurfs der **Richtlinien** für die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien)
- Prüfung neuer bzw. überarbeiteter **Errichtungsanordnungen** für polizeiliche Dateien (Anwendungen für besondere Einsatzlagen „BELA", Protokolldatei, Anwendungen auf Einzelplatzcomputer „EPC-Verfahren", Arbeitsdatei PIOS-Innere Sicherheit-APIS, Datei PSV, GAST-Dateien)
- Prüfung von **Dateimeldungen** (Asylbewerber, Telefonüberwachungen, GAST-Dateien)
- Mitwirkung im **Arbeitskreis Sicherheit** (INPOL-Neukonzeption, Datei „Gewalttäter Sport", bundesweites Meldesystem „fremdenfeindliche Straftaten", Datei „Schleuser")
- Auswertung der **Protokolldatei** (Abfragen im Zentralen Verkehrsinformationssystem – ZEVIS, im Informationssystem der Bayerischen Polizei (IBP), in INPOL-Bund-Dateien, im Ausländerzentralregister und in der Einwohnerdatei)
- **Bürgereingaben**

4.3 Allgemeine Prüfungen

Allgemeine Querschnittsprüfungen habe ich bei folgenden Polizeibehörden vorgenommen:

- Bayerisches Landeskriminalamt
- Polizeipräsidium München
- Präsidium der Bayerischen Grenzpolizei mit der Grenzpolizeiinspektion Waidhaus
- Polizeipräsidium Schwaben mit der Polizeidirektion Augsburg.

Aufgrund der Kontrollergebnisse kann ich feststellen, daß die bayerische Polizei mit personenbezogenen Daten **verantwortungsbewußt** und in aller Regel auch **datenschutzgerecht** umgeht. Verstöße gegen datenschutzrechtliche Bestimmungen bilden die Ausnahme.

4.3.1 Kriminalaktennachweis (KAN)

Meine Prüfungen der „Standarddatei" KAN haben gezeigt, daß die geprüfte Dienststelle die in früheren Tätig-

keitsberichten dargestellten datenschutzrechtlichen Erfordernisse überwiegend beachtet. Das im Vorjahr festgestellte hohe Datenschutzniveau hat die geprüfte Dienststelle noch nicht erreicht. Allerdings handelte es sich bei den beanstandeten Speicherungen teilweise um Altfälle, die nach früheren Richtlinien bearbeitet worden waren.

Im Berichtszeitraum habe ich nach folgenden Prüfansätzen vor Ort schwerpunktmäßig geprüft: Beleidigung, Beförderungserschleichung, fahrlässige Körperverletzung, Ladendiebstahl, Betrug, bestimmte Ordnungswidrigkeiten, Straftaten eines ausgewählten Monats, bestimmte Straftatenschlüssel (z.B. 0005 = sonstige polizeiliche Gefahrenabwehr), bestimmte Zeitpunkte für Aussonderungsprüfungen, bestimmte Erfassungszeiträume, Speicherungen sog. personenbezogener Hinweise (z.B. POLT = politisch motivierter Täter), Speicherungen sog. KAN-Merker (z.B. planmäßige überörtliche Begehung), die eine bundesweite Abrufbarkeit bewirken, Speicherungen von Kindern, Speicherungen von über 70jährigen Tatverdächtigen.

Die einzelnen Speicherungen, die nach den vorgenannten Kriterien ausgewählt wurden, habe ich nach folgenden **Maßstäben** geprüft:

- Sind die Speicherungen im KAN zur Gefahrenabwehr oder Strafverfolgung **erforderlich**? Läßt sich die Erforderlichkeit aus den polizeilichen Unterlagen nachvollziehen?
- Ist die **Speicherungsebene** (Regional-, Landes-, Bundes-KAN) richtig gewählt?
- Ist die **Dauer** der Speicherung auf das erforderliche Maß beschränkt? Insbesondere: Sind die durch Art. 38 Abs. 2 Satz 3 PAG vorgegebenen **Prüfungstermine** eingehalten?
- Sind in Fällen geringerer Bedeutung **kürzere Prüffristen** festgesetzt?
- Wurden die Prüfungstermine durch automatisierte Vergabe oder – wie von mir gefordert – durch **Sachbearbeiterentscheidung** festgesetzt?
- Wurde der **Ausgang des Strafverfahrens** berücksichtigt, insbesondere in Fällen, in denen der Tatverdacht entfallen war, eine Straftat nicht vorlag oder sich der Tatvorwurf geändert hatte? Ist die Prüfung durch den Sachbearbeiter **dokumentiert** und ist ggf. die Löschung, Fristverkürzung oder Aktualisierung des Tatvorwurfs vorgenommen worden?
- Sind bei der Speicherung von **Kindern** und über **70-jährigen** Tatverdächtigen die besonderen Anforderungen an die Speicherung berücksichtigt?
- Sind die Vergabe von **KAN-Merkern** und die damit verbundene Speicherung im Bundes-KAN sowie die Vergabe **personengebundener Hinweise** zutreffend und in den polizeilichen Unterlagen nachvollziehbar **dokumentiert?**

Festgestellte Mängel

Bei der von mir geprüften Polizeidirektion war in einer Reihe von Fällen die Festlegung des **Aussonderungsprüfdatums** (APD) nicht aus der Kriminalakte, sondern nur aus dem KAN ersichtlich. Ursache dafür war die automatisierte Vergabe des APD anstelle der erforderlichen Sachbearbeiterentscheidung, die für eine individuelle Beurteilung des Vorgangs unerläßlich ist. Folge kann sein, daß die Vorgänge **zu lange gespeichert** werden. Bei einzelnen Speicherungen war nicht nachzuvollziehen, warum sie zur polizeilichen Aufgabenerfüllung **erforderlich** waren.

Gerügt habe ich auch die Speicherung von Sachverhalten im KAN, bei denen es sich offensichtlich um **rein privatrechtliche Angelegenheiten** handelte und **kein Straftatenverdacht** vorlag. So wurde eine Person wegen Verdachts des Hausfriedensbruchs im KAN für 10 Jahre gespeichert. Bei näherer Prüfung des Vorgangs stellte sich heraus, daß der „Beschuldigte" eine Wohnung bewohnte, ohne die monatliche Miete zu bezahlen. Als Begründung für seine Weigerung hatte der Mieter das Fehlen eines Mietvertrages angegeben. Das staatsanwaltschaftliche Ermittlungsverfahren war gemäß § 376 StPO wegen fehlenden öffentlichen Interesses an einer öffentlichen Klage eingestellt worden.

In einer anderen Sache hatte der Besitzer einer Videothek seiner Forderung nach Rückgabe eines Videofilms und eines ausgeliehenen Videogeräts sowie der Zahlung der Leihgebühr mit einer Strafanzeige wegen Unterschlagung nachgeholfen. Das Verfahren wurde nach Erledigung eingestellt. Auch in diesem Fall ist das Vorliegen einer Straftat mehr als fraglich, eine 10jährige Speicherung im KAN jedenfalls verfehlt.

Auch bei der Vergabe sog. **personengebundener Hinweise** (PHW) habe ich Mängel festgestellt:

- So war der **PHW „POLT"** (politisch motivierter Täter) vergeben worden, obwohl er zum Zeitpunkt der Vorgangserfassung nicht mehr vergeben werden durfte.
- Auch der **PHW „ANST"** (Ansteckungsgefahr) wird nicht immer mängelfrei vergeben. In einem Fall war die Grundlage der Speicherung im Vorgang nicht nachvollziehbar dokumentiert.
- **Fehlende Dokumentation** der Erforderlichkeit der Speicherung stellte ich auch beim PHW „FREI" (Freitodgefahr) fest. In diesem Fall war auch noch der PHW „HELA" (war bereits in Heilanstalt) vergeben worden, der bereits seit 1990 nicht mehr zulässig ist.

Die von mir gerügten Mängel wurden von der Polizei zwischenzeitlich bereinigt.

Für noch akzeptabel halte ich die Vergabe des **PHW „GEKR"** (geisteskrank) in zwei Fällen, obwohl die in der Dienstanweisung geforderte **ärztliche Feststellung**

einer Geisteskrankheit nicht vorlag. Die Bemerkung auf der Rückseite eines ärztlichen Untersuchungsberichts anläßlich einer Blutalkoholuntersuchung, der Proband sei geisteskrank, reicht als Grundlage für die ärztlich gesicherte Annahme von Geisteskrankheit nicht aus. In diesem Fall konnte die Polizei die Speicherung jedoch auf Angaben von Verwandten und Anstaltsärzten stützen.

Im zweiten Fall belegte die Einlieferung in ein Nervenkrankenhaus durch die Polizei noch keine Geisteskrankheit; aber auch hier traten weitere, tragfähige Erkenntnisse hinzu.

4.4 Bayerisches Landeskriminalamt (BLKA)

Im Berichtsjahr habe ich wieder schwerpunktmäßig die „Arbeitsdatei PIOS Innere Sicherheit" (APIS) geprüft. Ferner habe ich wie im Vorjahr die Arbeitsdatei „Organisierte Kriminalität" (ADOK) sowie besondere Mittel der Datenerhebung (Polizeiliche Beobachtung) überprüft.

4.4.1 APIS

Ein Schwerpunkt der Prüfung waren wie in den Vorjahren die sog. anderen Straftaten und der ausgewählte Suchbegriff „Wahl". **„Andere Straftaten"** sind nach der APIS-Richtlinie solche Straftaten, bei denen Anhaltspunkte vorliegen, daß damit eine staatsfeindliche Zielsetzung verfolgt wird. Ferner habe ich eine Vielzahl **ausgewählter Namen,** darunter auch Namen von Personen, die in der bereits gelöschten Datei „MWG '92" des Polizeipräsidiums München gespeichert waren, auf Bestand in APIS geprüft. Außerdem habe ich geprüft, ob Speicherungen unter der APIS-Kategorie **„Verdächtige Personen"** rechtmäßig waren.

Die Prüfung führte zu folgendem Ergebnis:

- APIS ist in einem datenschutzrechtlich guten Zustand.
- In wenigen Fällen war die **Notwendigkeit der Speicherung** (APIS-Relevanz) auch nach Einsicht in die dazugehörenden Unterlagen nicht zu erkennen.

APIS-Relevanz der gespeicherten Beleidigungen und der Speicherungen unter dem Suchbegriff „Wahl"

Bei der Speicherung von Personen wegen Beleidigungsdelikten war die **staatsfeindliche Zielsetzung nicht immer zu erkennen.** Zwar hatten die Beleidigungen regelmäßig politischen Bezug; dies reicht für sich allein jedoch für eine Speicherung in APIS nicht aus. Diese Feststellung mußte ich ausschließlich bei solchen Beleidigungen treffen, die schon mehrere Jahre (Tatzeit 1988) zurückliegen. Bei Beleidigungen aus jüngerer Zeit (Tatzeit 1993), die überwiegend von rechtsextremistischen Tätern begangen worden waren, war der staatsfeindliche Bezug hingegen nachvollziehbar.

Die unter dem Suchbegriff „Wahl" stichprobenartig geprüften Fälle genügten, mit einer Ausnahme den datenschutzrechtlichen Anforderungen. Eine Person war gespeichert worden, weil sie eine **nichtangemeldete Versammlung** und eine weitere Versammlung **abweichend von dem im Auflagenbescheid** der Kreisverwaltungsbehörde festgelegten Versammlungsort durchgeführt hatte. Ich habe gebeten, die Notwendigkeit der weiteren Speicherung unter Berücksichtigung der Justizentscheidung zu überprüfen.

Aufnahme von Störern des Weltwirtschaftsgipfels

Personen, die in der Datei „Münchner Weltwirtschaftsgipfel 1992" gespeichert waren, wurden in APIS nur aufgenommen, wenn gegen sie der Verdacht der **Nötigung** oder **Verunglimpfung** des Staates bestand. Die Personen stehen in Verdacht, die Begrüßungszeremonie am 6. Juli 1992 anläßlich des Weltwirtschaftsgipfels auf dem Max-Joseph-Platz in München durch den Gebrauch von Trillerpfeifen und ohrenbetäubendes Schreien massiv gestört zu haben, um hierdurch den geordneten Ablauf der Begrüßungszeremonie (u.a. das Abspielen der Nationalhymnen) zu verhindern. Da der Abbruch der Veranstaltung bevorstand, wurden die gespeicherten Personen aus dem Kreis der friedlichen Zuschauer herausgedrängt und später festgenommen. Die Speicherung in APIS bis zum Abschluß des Strafverfahrens halte ich für gerechtfertigt, zumal es sich um sog. Katalogstraftaten handelt. Danach wird unter Berücksichtigung der Justizentscheidung die Erforderlichkeit der weiteren Speicherung zu prüfen sein.

Aussonderungsprüffrist bei mehreren Speicherungen

Ist eine Person mit **mehreren** APIS-relevanten Ereignissen von jeweils unterschiedlicher Speicherungsdauer in APIS erfaßt, so wurde bisher vom BLKA jedes einzelne Ereignis mit einer eigenen Speicherungsfrist versehen und gesondert auf weitere APIS-Relevanz überprüft. Das BLKA hat auf den hohen personellen Aufwand, der mit dieser Speicher- und Prüfungspraxis verbunden ist, hingewiesen. Hier hat das BLKA unnötigerweise zu viel Mühe aufgewandt. Entsprechend der Regelung in Art. 38 Abs. 2 Satz 5 Polizeiaufgabengesetz ist eine „Zwischenprüfung" von Speicherungen dann **nicht erforderlich,** wenn zu der gleichen Person weitere APIS-relevante Erkenntnisse bestehen, die eine längere Speicherung in APIS erfordern. Entscheidend für die Festsetzung der (Gesamt-)Aussonderungsprüffrist für alle Erkenntnisse zu einer Person ist danach die APIS-relevante Speicherung mit dem **fernsten Aussonderungsprüfdatum.** Auch die Neufassung der Errichtungsanordnung zur Datei APIS vom 8. Februar 1993 hat diese datenschutzrechtlich unbedenkliche Sichtweise aufgegriffen.

4.4.2 Arbeitsdatei „Organisierte Kriminalität-ADOK"

Aufgabenstellung und Zweck dieser Datei habe ich im 14. Tätigkeitsbericht eingehend dargestellt und erläutert (Ziff. 4.6.2). Im Berichtszeitraum habe ich diese Datei wiederum einer Prüfung unterzogen.

Schwerpunkte waren

- die Dokumentation von Telefonüberwachungsmaßnahmen in der Datei und
- die Speicherung sog. „anderer Personen" (Kontaktpersonen).

Datenschutzrechtliche Verstöße habe ich nicht festgestellt. Lediglich in einem Fall waren die Gründe für die Verlängerung der Speicherung einer „anderen Person" **nicht ausreichend dokumentiert.** Als **„andere Person"** ist eine Person definiert, die weder Beschuldigter, Verdächtiger, Gefährdeter oder Geschädigter ist, aber mit Beschuldigten oder Verdächtigen oder Organisationen in Verbindung steht und bei der ausreichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß die Erfassung zur Aufklärung oder Bekämpfung einer Straftat von erheblicher Bedeutung erforderlich ist.

4.4.3 Polizeiliche Beobachtung

Die Polizei kann personenbezogene Daten, insbesondere die Personalien einer Person sowie das amtliche Kennzeichen des von ihr benutzten Kraftfahrzeugs, zur polizeilichen Beobachtung ausschreiben, wenn

1. die Gesamtwürdigung der Person und ihrer bisher begangenen Straftaten erwarten lassen, daß sie auch künftig Straftaten von erheblicher Bedeutung begehen wird oder
2. Tatsachen die Annahme rechtfertigen, daß die Person Straftaten von erheblicher Bedeutung begehen wird,

und die polizeiliche Beobachtung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist. Wird die Person oder das Kraftfahrzeug angetroffen, so können Erkenntnisse über das Antreffen sowie über Kontakt- und Begleitpersonen und mitgeführte Sachen an die ausschreibende Polizeidienststelle übermittelt werden.

Überprüft habe ich die Rechtmäßigkeit

- der **Anordnung** gemäß Art. 36 Abs. 1 PAG sowie
- der **Verlängerung der Laufzeit** gemäß Art. 36 Abs. 3 Satz 3 PAG.

In allen geprüften Fällen lagen die Voraussetzungen für eine (erneute) Ausschreibung zur polizeilichen Beobachtung vor.

4.5 Polizeipräsidium München

Beim Polizeipräsidium München habe ich in einer mehrtägigen Prüfung folgende Bereiche kontrolliert:

- die Datei Kriminalaktennachweis (KAN) mit dazugehörigen Akten
- die Datei PSV mit dazugehörigen Unterlagen
- die SPUDOK-Datei Kraftfahrzeuge, Boote, Luftfahrzeuge
- verschiedene GAST-Dateien auf APC
- die Lichtbild-Vorzeigekartei und das sog. „Bekannte-Täter-Verfahren" (BT-Verfahren) sowie
- die Personenkartei „Psychisch Kranke oder Psychisch Gestörte".

Darüber hinaus waren auch der Polizeieinsatz vom 13. Februar 1991 vor der Bayerischen Börse und die in diesem Zusammenhang von der Polizei erhobenen Daten Gegenstand meiner datenschutzrechtlichen Prüfung.

Als Ergebnis konnte ich bei der Datenverarbeitung des Polizeipräsidiums München nur wenige, nicht gravierende Mängel feststellen.

4.5.1 Kriminalaktennachweis (KAN)

Die stichprobenartige Prüfung von KAN-Speicherungen und der dazugehörigen Kriminalakten habe ich, wie bei anderen Polizeidienststellen, anhand spezieller Prüfkriterien durchgeführt. Der geprüfte Akten- und Dateibestand vermittelte einen **positiven Gesamteindruck.**

Allerdings war festzustellen: Bis zur Umsetzung der Dienstanweisung KAN vom 24. Oktober 1990, die sich wegen notwendiger Erörterungen mit dem Innenministerium bezüglich der Auflösung des Regional-KAN verzögerte, wurden **Fälle der polizeilichen Gefahrenabwehr** noch bis Februar 1992 **für 10 Jahre** im Regional-KAN gespeichert, obwohl es sich hierbei grundsätzlich um Fälle von geringerer Bedeutung handelte, für die in der Regel eine Speicherungsdauer von 5 Jahren ausreichend ist. Ich habe um Bereinigung gebeten.

Das Polizeipräsidium hat eine Verkürzung der Fristen für die Altfälle zugesagt, wenn sie mit vertretbarem Aufwand möglich ist.

Die **Datei Münchner Weltwirtschaftsgipfel (MWG '92)** wurde zum 1. März 1993 gelöscht. Damit fielen aber die Speicherungen in anderen Dateien nicht weg. So hat meine KAN-Prüfung ergeben, daß von 18 Personen, die von mir überprüft wurden, 11 Personen Bestand im KAN (sowohl Regional-KAN wie auch Landes-KAN) hatten. Eine dieser Personen war nicht wegen der Vorgänge im Zusammenhang mit dem Weltwirtschaftsgipfel im KAN gespeichert. 3 Personen waren vorläufig im Regional-KAN des Polizeipräsidiums gespeichert, da die polizeilichen Ermittlungen zum Prüfungszeitpunkt noch nicht abgeschlossen waren. Die restlichen Personen waren im Zusammenhang mit Straftaten im KAN gespeichert, die bei den Vorgängen am 6. Juli 1992 auf dem Münchner Max-Joseph-Platz begangen worden waren. Die Personen wurden wegen Verdachts der versuchten Nötigung, der Verunglimpfung des Staates und seiner Symbole und des Widerstandes gegen Vollstreckungsbeamte angezeigt, so daß zumindest von einem Anfangstatverdacht auszugehen ist. Verfahrensausgänge lagen in den geprüften Fällen noch nicht vor. Datenschutzrechtliche Bedenken gegen die Speicherungen bestehen nicht.

4.5.2 Datei Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)

Das Ballungsraumverfahren wurde zwischenzeitlich weitgehend an die Vorgaben der Errichtungsanordnung/Dienstanweisung der Datei PSV (EA/DA PSV) angepaßt. Die Datei wird ganz überwiegend datenschutzgerecht geführt.

Folgende Verbesserungen habe ich gefordert:

- **Berücksichtigung der KAN-Löschung in der PSV**

  Sind im Kriminalaktennachweis zu einem Vorgang mehrere Täter gespeichert, so sind diese Personen in der PSV unter der Rubrik „Beschuldigte, Betroffene" gespeichert. Wurde jedoch später die Kriminalakte über einen dieser „Mittäter" wegen Fristablaufs vernichtet, so wurde diese Person zwar im KAN gelöscht. In der PSV wurde sie jedoch **weiterhin unter der negativen Rubrik** „Beschuldigte, Betroffene" gespeichert, wenn und solange ein „Mittäter" im KAN gespeichert blieb.

  Diese Speicherung unter der negativen Rubrik „Beschuldigte, Betroffene" ist nicht sachgerecht, da einer aus dem KAN gelöschten Person der Status „Beschuldigter, Betroffener" nicht mehr zukommt. Eine solche Speicherung in der PSV ist belastend und kann zu Nachteilen führen.

  Das Polizeipräsidium hat mir Berücksichtigung zugesagt.

- **Löschprogramm für Speicherung von Kindern**

  Unterlagen über Kinder, die in der PSV gespeichert sind, werden nach 2 Jahren vernichtet. Die dazugehörenden Dateispeicherungen konnten jedoch bisher nicht gelöscht werden, da ein entsprechendes Löschprogramm fehlte. Ich habe deshalb die alsbaldige Erstellung eines Löschprogramms für Kinder gefordert.

  Das Polizeipräsidium hat das Programm inzwischen erstellt und fällige Löschungen durchgeführt. Künftig wird die Speicherung von Kindern in der PSV grundsätzlich nach 2 Jahren gelöscht.

- **Rückmeldung bei Wegfall des Tatverdachts bei Ordnungswidrigkeiten**

  Ordnungswidrigkeiten werden von der Polizei bei der Verfolgungsbehörde (z.B. beim Kreisverwaltungsreferat) angezeigt. Entfällt jedoch nach Abschluß des Verfahrens bei der Verfolgungsbehörde der Tatverdacht, so wird bisher dieser Umstand nicht an die Polizei gemeldet, so daß der Betroffene weiterhin im KAN gespeichert bleibt. Diese Praxis galt bisher in ganz Bayern. Hier sollte wenigstens bei Ordnungswidrigkeiten, die im Landes-KAN gespeichert sind, eine **ähnliche Regelung wie bei den Strafverfahren** angestrebt werden (Rückmeldung an die Polizei bei Wegfall des Tatverdachts, damit die Eintragung im KAN gelöscht werden kann).

  Diese Frage ist inzwischen vom Innenministerium insoweit geklärt, als bezüglich der Speicherungen im Landes-KAN bei Wegfall des Tatverdachts eine **Rückmeldung von der Bußgeldbehörde an die Polizei veranlaßt** wird.

- **Speicherung von Versammlungsvorgängen in der PSV**

  Nach der Errichtungsanordnung/Dienstanweisung für die Datei PSV (EA/DA PSV) sind Vorgänge im Zusammenhang mit der **polizeilichen Betreuung von Versammlungen** nicht in der Datei PSV zu speichern.

  Das Polizeipräsidium hält die Speicherung **aller** Versammlungen in der Datei PSV, **bei denen das Dezernat „Staatsschutz" eingesetzt** war, für notwendig. Ein Einsatz erfolge nur in den Fällen, in denen eine Gefahrenprognose ergebe, daß von der Veranstaltung eine Gefahr ausgehen oder für die Veranstaltung eine Gefahr drohen könne. Die Speicherung von Versammlungen sei zur Lagebeurteilung und zur Gefahrenprognose für zukünftige Fälle auch dann erforderlich, wenn diese – entgegen der ursprünglichen polizeilichen Einschätzung – störungsfrei verlaufen seien.

  Die Frage, welche Veranstaltungen und Versammlungen in der PSV gespeichert werden dürfen, bedarf noch der Erörterung mit dem Innenministerium.

4.5.3 Datei „Delikte rund um das Kfz" im EDV-System SPUDOK

Die Datei dient der Bekämpfung der organisierten Kfz-Verschiebung sowie von deren Begleitdelikten. Datenschutzrechtliche Bedenken gegen die Führung und Nutzung dieser Datei bestanden nicht.

4.5.4 Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten – GAST-Dateien

GAST-Dateien habe ich diesmal in erster Linie auf **„Freitexte"**, die nicht von der Errichtungsanordnung gedeckt sind, kontrolliert. Darüber hinaus habe ich nach **„schwarzen Listen oder Verzeichnissen"** mit personenbezogenen Daten gesucht, die von polizeilichen Mitarbeitern angelegt hätten werden können. Weder das eine noch das andere habe ich anläßlich meiner Kontrolle feststellen können. Ich halte es auch nahezu für ausgeschlossen, daß einzelne Mitarbeiter unbemerkt „schwarze Listen" anlegen können. Denn jede Dienststelle wird durch einen eigenen EDV-Fachmann **betreut**, der jederzeit Zugriff auf alle von den Mitarbeitern der Dienststelle betriebenen Dateien besitzt und in unregelmäßigen Abständen die „Inhaltsverzeichnisse" der Systeme auf solche Listen überprüft. Spätestens zu diesem Zeitpunkt würden „versteckte" Speicherungen entdeckt.

4.5.5 Lichtbild-Vorzeigekartei

In dieser Kartei werden Personen gespeichert,

- die als Beschuldigte oder Tatverdächtige einer strafbaren Handlung erkennungsdienstlich behandelt wurden und
- bei denen aufgrund bestimmter Anhaltspunkte zu vermuten ist, daß sie in gleicher oder ähnlicher Weise erneut auftreten werden.

Die Kartei dient der **Fahndung nach unbekannten Tätern.** Hauptanwendungsbereich ist die Lichtbildsuche. Dabei wird unter Berücksichtigung der von Zeugen angegebenen Beschreibungsmerkmale geprüft, ob sich aus den im System gespeicherten Personen der Gesuchte identifizieren läßt.

In der Kartei waren zum Prüfungszeitpunkt rund 43.000 Personen mit Lichtbildern erfaßt; darunter befanden sich auch 13 Kinder zwischen 10 und 14 Jahren sowie 72 Personen, die älter als 70 Jahre waren. Die Dauer der Speicherung in der Kartei richtet sich nach der Dauer der Speicherung im Kriminalaktennachweis. Die von mir stichprobenartig überprüften Fälle gaben keinen Anlaß für Beanstandungen.

Seit 1. September 1993 gehört die EDV-unterstützte **manuelle** Führung der Lichtbildkartei der Vergangenheit an. Sie wurde durch ein **digitalisiertes Bildverarbeitungssystem** ersetzt. Dieses System habe ich am 7. September 1993 besichtigt und grundsätzlich positiv beurteilt. Das neue System erleichtert die Arbeit der Polizei und die Aufgaben des Zeugen, stellt aber **aus datenschutzrechtlicher Sicht keine wesentliche qualitative Änderung** im Vergleich zum bisherigen Verfahren dar. Ich werde aber im nächsten Jahr – mit Hilfe des neuen Systems – eine deliktsorientierte Kontrolle des Umfangs der erkennungsdienstlichen Behandlung durchführen.

4.5.6 Personenkartei „Psychisch Kranke oder Psychisch Gestörte"

Die Kartei dient der Sammlung und Auswertung von Erkenntnissen über Personen, die psychisch krank oder psychisch **gestört sind** oder die nach ihrem Auftreten, Verhalten und Persönlichkeitsbild **dafür gehalten werden müssen** und bei denen der Verdacht besteht, daß sie durch krankheitsbedingte Handlungen die **öffentliche Sicherheit und Ordnung stören können.** Gespeichert werden Personen,

- die durch krankheitsbedingte Handlungen die öffentliche Sicherheit und Ordnung, insbesondere das **eigene Leben** oder die **eigene Gesundheit,** gefährdeten oder
- die rechtswidrige Taten/Ordnungswidrigkeiten begingen,

und der Verdacht besteht, daß sie in gleicher oder ähnlicher Weise auftreten können.

Die Datei dient der polizeilichen Aufgabenerfüllung, insbesondere dem **Schutz des Betroffenen** und **anderer Personen** sowie der **besseren Beurteilung der Glaubwürdigkeit von Zeugen** und **Anzeigeerstattern.** Dies erleichtert der Polizei den sachgerechten Einsatz von Personal- und Sachmitteln (z.B. bei Mitteilung von Unglücksfällen) und die Auswahl verhältnismäßiger Maßnahmen.

Die Aufbewahrungsdauer der einzelnen Karteiblätter, die beim Kriminaldauerdienst abgelegt sind, beträgt maximal **2 Jahre,** gerechnet vom Zeitpunkt des letzten Ereignisses.

Eine solche Datei ist aus meiner Sicht nicht unproblematisch. Während für die Vergabe des personengebundenen Hinweises „geisteskrank" im Kriminalaktennachweis in der Regel eine ausreichende **ärztliche Feststellung** vorliegen muß, ist dies für die Aufnahme in die Kartei nicht der Fall. In einigen der geprüften Fälle konnte ich die **Erforderlichkeit** der Speicherung **nicht nachvollziehen.**

Das Polizeipräsidium macht geltend: Da nur in wenigen Fällen ein „ärztliches Gutachten" die Aufnahme von Personen in diese Kartei (zweifelsfrei) begründe, obliege es dem **jeweiligen Sachbearbeiter,** eigenverantwortlich die Bewertung des Persönlichkeitsbildes vorzunehmen. Dabei könne sich – ergänzt durch weitere Hinweise oder Recherchen bzw. anhand bestehender Unterlagen (KpS-Vorgänge, mitgeführte Papiere/Schreiben/Urkunden usw.) – ein Gesamtbild für den Beurteiler ergeben. Da diese Details aus einer Karteikarte nicht hervorgingen, sei die Speicherung nur für Außenstehende nicht nachvollziehbar.

Nach der Stellungnahme des Polizeipräsidiums beabsichtige ich, mit dem Innenministerium ein Gespräch über die **Notwendigkeit** und die **Voraussetzungen** einer solchen Datei zu führen.

4.5.7 Überprüfung der Speicherung personenbezogener Daten von Demonstranten vor der Bayerischen Börse in München am 13. Februar 1991

Aufgrund eines Presseberichts über einen Polizeieinsatz am 13.Februar 1991 vor der Bayerischen Börse, bei dem 26 Frauen vorläufig festgenommen und erkennungsdienstlich behandelt wurden, habe ich die Speicherung der personenbezogenen Daten dieser Frauen überprüft.

Die Frauen hatten vor der Bayerischen Börse gegen den Golfkrieg und die „Männerherrschaft" demonstriert und dabei die Eingangstüre mit einem Fahrradschloß verschlossen, wobei sie den Schlüssel im Schloß stecken ließen. Der Anfangsverdacht strafbarer Handlungen war von Polizei und Staatsanwaltschaft bejaht, und deshalb Strafverfahren eingeleitet worden. Die Speicherungen waren deshalb aus datenschutzrechtlicher Sicht im Hinblick auf Art. 38 Abs. 2 PAG nicht zu beanstanden. Danach kann die Polizei 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. Diese Voraussetzungen waren zum Zeitpunkt meiner Prüfung gegeben.

Nachdem aber eine Teilnehmerin vom Bayerischen Obersten Landesgericht rechtskräftig vom Vorwurf der Nötigung **freigesprochen** worden war, habe ich die Polizei zur Prüfung der Rechtmäßigkeit der weiteren Speicherung aufgefordert, da nach meiner Einschätzung der Tatverdacht und damit die Voraussetzungen für die weitere Speicherung entfallen sind. Die personenbezogenen Unterlagen der betroffenen Teilnehmerin wurden daraufhin von der Polizei vernichtet. Wegen der Speicherung der anderen Demonstrationsteilnehmerinnen habe ich die Polizei um Überprüfung vergleichbarer Fälle gebeten. Die Antwort steht noch aus.

4.6 Bayerische Grenzpolizei

Bei der Bayerischen Grenzpolizei habe ich in einer mehrtägigen Prüfung eine datenschutzrechtliche Kontrolle einer Grenzpolizeiinspektion sowie der nachgeordneten Grenzpolizeistation vorgenommen.

Folgende Bereiche waren Gegenstand meiner Prüfung:

- die Datei Grenzaktennachweis (GAN)
- die Datei „Grenzüberschreitender Lkw- und Omnibusverkehr (G-LKW/BUS)"
- die SPUDOK-Datei „Gefälschte Dokumente – DOKU-GPP"
- die SPUDOK-Datei „Organisierte Kriminalität im grenzüberschreitenden Verkehr – OK-GV/GPP"
- verschiedene GAST-Dateien sowie
- eine spezielle EDV-Anwendung der Grenzpolizei zur Identifizierung von entwendeten bzw. unterschlagenen Kraftfahrzeugen.

Bei der Prüfung habe ich keine gravierenden Mängel festgestellt.

Grenzaktennachweis (GAN)

Für die Bayerische Grenzpolizei wird zur Erfüllung der ihr obliegenden Grenzaufgaben (Art. 5 Abs. 1 Polizeiorganisationsgesetz) die Datei Grenzaktennachweis (LGAN) beim Bayer. Landeskriminalamt geführt. Im LGAN werden geführt:

- die in der Errichtungsanordnung KAN genannten Daten
- sicherheitsgefährdende Verstöße im grenzüberschreitenden Lkw- und Omnibusverkehr
- Daten aus grenzpolizeilichen Maßnahmen mit erheblichem Rechtseingriff (belastende Verwaltungsakte).

Die in der Errichtungsanordnung KAN genannten Daten werden bei Speicherungen in den GAN automatisch in den Landes-KAN übernommen.

Bei der Speicherung grenzspezifischer Maßnahmen (Daten aus grenzpolizeilichen Maßnahmen mit erheblichem Rechtseingriff wie z.B. Zurückweisung, Abschiebung) wurde bisher durch die Vergabe eines speziellen Merkers sichergestellt, daß diese Speicherungen für Dienststellen der Bayer. Landespolizei nicht zur Verfügung stehen. Diese differenzierte Zugangsberechtigung ist nunmehr aufgehoben worden. Die Änderung wurde nach Mitteilung des Innenministeriums erforderlich, da den Dienststellen der Bayerischen Landespolizei durch die Änderung des Asylverfahrensgesetzes zum 1. Juli 1993 Aufgaben im Zusammenhang mit der Zurückschiebung von Asylbewerbern, die über sichere Drittstaaten unerlaubt eingereist sind, übertragen wurden. Deshalb müsse die Landespolizei zur Vorbereitung der Entscheidung der Ausländerbehörde über die Zurückschiebung auch auf die im Landes-GAN enthaltenen Erkenntnisse (z.B. Zurückweisungen an der Grenze) zurückgreifen können.

Um das erweiterte rechtliche Instrumentarium der Zurückschiebung von Asylbewerbern in der polizeilichen Praxis verwenden zu können, muß der Polizei die Möglichkeit gegeben werden, bereits vorhandene Erkenntnisse auszuwerten. Grundsätzliche datenschutzrechtliche Bedenken gegen die **erweiterte Zugriffsbefugnis für die Beamten** der Landespolizei bestehen deshalb nicht.

Der **Schwerpunkt** meiner datenschutzrechtlichen Prüfung im GAN-Bereich lag bei der Kontrolle der den Speicherungen zugrundeliegenden **Kriminalakten** der Grenzpolizeiinspektion.

Zur stichprobenartigen Prüfung von GAN-Speicherungen und der dazugehörigen Akten habe ich folgende Bereiche ausgewählt:

- Speicherungen von Kindern zwischen 10 und 14 Jahren
- Speicherungen von Personen über 70 Jahre
- Sachverhalte mit einer bestimmten Tatzeit und einem bestimmten Aussonderungsprüfdatum
- Sachverhalte mit einem bestimmten GAN-Schlüssel (z.B. sonstige grenzpolizeiliche Gefahrenabwehr 000031) und
- bestimmte KAN-Merker (z.B. gewohnheits- und gewerbsmäßige Begehung).

Bei der Prüfung habe ich keine Speicherungen festgestellt, die im GAN nicht hätten erfaßt werden dürfen. In einzelnen Fällen fehlte die **Angabe des Aussonderungsprüfdatums (APD)** in der jeweiligen Kriminalakte (fehlende Sachbearbeiterentscheidung) und die Dokumentation des **Verfahrensausgangs.** In einem Fall war das APD fehlerhaft festgelegt worden. Zu begrüßen ist, daß die Grenzpolizei in zahlreichen Fällen von der Möglichkeit der **Vergabe verkürzter Aussonderungsprüffristen** Gebrauch gemacht hat.

Die **Aktenführung** könnte aus datenschutzrechtlicher Sicht noch verbessert werden:

Es fehlt an einer **nach Personen getrennten Führung der Kriminalakten.** Statt dessen wurde

auch bei mehreren Tatbeteiligten nur **eine** Kriminalakte angelegt. Diese Aktenführung ist **datenschutzrechtlich bedenklich,** weil bei einem erneuten Auftreten einzelner Beteiligter (was u.U. eine Verlängerung der Speicherungsdauer zur Folge haben kann) die Gefahr besteht, daß auch die „Akten" der anderen Beteiligten **länger als erforderlich aufbewahrt werden.** Das Präsidium der Grenzpolizei hat mir zugesagt, die Aktenführung zu ändern.

Handschriftliche Notizen der Sachbearbeiter, die zur Kriminalakte genommen waren, wiesen auf der Rückseite zum Teil personenbezogene Daten anderer Beschuldigter auf, die in keinem Zusammenhang mit den geprüften Akten standen. Auf Nachfrage wurde mir erklärt, daß dies aus Gründen der Papierersparnis angeordnet worden sei. Zwischenzeitlich werde diese Art der „Altpapierverwertung" nicht mehr praktiziert.

Datei „Grenzüberschreitender LKW- und Omnibusverkehr (G-LKW/Bus)"

In dieser Datei werden von der Grenz- und der Landespolizei **sicherheitsgefährdende Verstöße ausländischer Unternehmen** im grenzüberschreitenden LKW- und Omnibusverkehr erfaßt. Sie erleichtert der Polizei das Erkennen von Wiederholungstätern, die sicherheitsgefährdende Verstöße gegen Vorschriften zum Schutz der Sicherheit im Straßenverkehr begangen haben und ermöglicht damit die Durchführung geeigneter, einzelfallbezogener Maßnahmen, bis hin zum Einreiseverbot.

Gravierende datenschutzrechtliche Mängel habe ich nicht festgestellt. Lediglich in zwei Fällen fehlte die Angabe des **Verfahrensausgangs** sowie die Angabe des **Aussonderungsprüfdatums** in der Akte.

SPUDOK-Datei „Gefälschte Dokumente (DOKU-GPP)"

Die Datei dient der Bekämpfung der mißbräuchlichen Verwendung gefälschter Ausweispapiere, Aufenthaltsgenehmigungen, Paßkontrollstempel sowie sonstiger gefälschter Dokumente. Zu diesem Zweck werden in der Datei gespeichert,

- Personen, bei denen der **Verdacht der Urkundenfälschung** oder des Mißbrauchs von Ausweisen vorliegt, sowie
- Personen, die der **Teilnahme** an solchen Straftaten verdächtig sind.

Ferner werden auch Institutionen, die in Verdacht stehen, Beihilfe zu Urkundsdelikten zu leisten, gespeichert.

Die von mir geprüften Speicherungen gaben keinen Anlaß für Beanstandungen.

SPUDOK-Datei „Organisierte Kriminalität im grenzüberschreitenden Verkehr (OK-GV/GPP)"

Die Datei dient – insbesondere im Bereich der organisierten Kriminalität – dem Erkennen von Tatzusammenhängen und Täterverbindungen, die bei der Auswertung von Strafanzeigen und Mitteilungen aus den Deliktsbereichen

- Einschleusung illegaler Ausländer (auch ohne Bezug zur organisierten Kriminalität)
- internationale Kfz-Verschiebungen sowie
- organisierte Diebes- und Hehlerbanden

gewonnen werden. Dazu ist es in Fällen der Schleuserkriminalität erforderlich, neben den Schleusern auch die **Geschleusten** zu erfassen. Die von anderen Datenschutzbeauftragten gepflegten datenschutzrechtlichen Bedenken gegen die Speicherung geschleuster Personen teile ich deshalb nicht.

Die von mir geprüften Datensätze entsprachen datenschutzrechtlichen Anforderungen.

Dateien im Rahmen der Errichtungsanordnung für Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten – GAST-Dateien

Derzeit sind 5 GAST-Dateien in Betrieb:

- Datei „Grenzübertrittsbescheinigung"
- Datei „Zurückweisung"
- Datei „Aktenzusammenführung"
- Datei „LP" (Suchdatei für abgelegte Anzeigen)
- Datei „Neuigkeitsbogen".

Ich halte diese Dateien zwar für erforderlich, habe aber um Prüfung gebeten, ob die Verfahren Aktenzusammenführung, Aktensuchdatei und Neuigkeitsbogen im Rahmen der Vorgangsverwaltung betrieben werden können. Zweck dieser Dateien ist in erster Linie die Verwaltung von Vorgängen und Sachverhalten und nicht die unmittelbare polizeiliche Gefahrenabwehr oder Strafverfolgung.

Außerdem genügten die **Löschungsregelungen** für alle Dateien wegen mangelnder Bestimmtheit nicht datenschutzrechtlichen Anforderungen. Die Grenzpolizei wird nach Einführung der Vorgangsverwaltungsdatei bei der GPS den Datenbestand der von mir bezeichneten drei GAST-Anwendungen dorthin übernehmen. Die Löschungsregelungen wurden überarbeitet.

EDV-Anwendung zur Identifizierung von entwendeten bzw. unterschlagenen Kraftfahrzeugen (FINAS)

Seit der Offnung der Grenzen zu den osteuropäischen Staaten sind die Diebstähle von Kraftfahrzeugen in der Bundesrepublik Deutschland und ganz Westeuropa erheblich angestiegen. Es wird davon ausgegangen, daß derzeit in Westeuropa jährlich ca. 1 Million Fahrzeuge abhanden kommen. Etwa 80 % dieser Fahrzeuge erhalten nach dem Diebstahl eine neue Identität. Um die polizeiliche Fahndung zu unterlaufen, wird dabei auch die Fahrzeugidentifizierungsnummer (FIN) gefälscht. Zur Fahndungsunterstützung hat die Grenzpolizei FINAS entwickelt und damit eine Vielzahl entwendeter bzw. unterschlagener Pkw sicherstellen können.

Ich habe mich davon überzeugen können, daß die Datei keine personenbezogenen Daten enthält.

4.7 Prüfung der Rechtmäßigkeit von Abfragen im Informationssystem der Bayerischen Polizei (Protokolldatei)

Auch im Berichtszeitraum 1993 habe ich die Rechtmäßigkeit von Abfragen in Informationssystemen, die der bayerischen Polizei zur Verfügung stehen, durch anlaßabhängige und anlaßunabhängige Auswertungen der Protokolldaten überprüft.

4.7.1 Anlaßunabhängige Auswertungen der Protokolldatei in verschiedenen DV-Anwendungen (KAN, Fahndung, ZEVIS, EWO, AZR)

In Bayern hat grundsätzlich jeder im Vollzugsdienst tätige Polizeibeamte Zugriff auf das Informationssystem der Bayerischen Polizei (IBP), die Bundes-(INPOL-)dateien, z.B. Kriminalaktennachweis, Fahndungsdatei, Haftdatei, Erkennungsdienstdatei, sowie auf die über IBP erschließbaren nichtpolizeilichen Dateien (derzeit Einwohnerdateien, Ausländerzentralregister, Zentrales Verkehrsinformationssystem). Damit stehen ihm umfangreiche personenbezogene Datensammlungen über eine Vielzahl von Personen zur Verfügung, die teilweise besonders sensible Informationen enthalten.

Die Daten unterliegen wegen ihrer besonderen Sensibilität strengen **Sicherheitsvorkehrungen.** So setzt der **Zugang** zum System die Eingabe der persönlichen **Kennung** des Polizeibeamten und eines individuellen **Paßwortes** voraus. Darüber hinaus werden alle Abfragen der Polizei in polizeilichen Informationssystemen oder in den erschließbaren nichtpolizeilichen Dateien in einer beim Landeskriminalamt geführten **Protokolldatei** so festgehalten, daß auch der **abfragende Polizeibeamte** festgestellt werden kann. Ich habe dadurch die Möglichkeit, durch Stichproben zu kontrollieren, ob der jeweilige Beamte die personenbezogenen Daten rechtmäßig, d.h. zur Erfüllung seiner polizeilichen Aufgaben, abgefragt hat. Anlaßunabhängige Auswertungen sind nicht Ausdruck eines generellen Mißtrauens gegenüber der Polizei, sondern dienen der Vorsorge gegen den möglichen Mißbrauch polizeilicher Auskunftssysteme für polizeifremde oder gar kriminelle Zwecke.

Ich habe deshalb auch in diesem Berichtszeitraum Auswertungen der Protokolldatei vorgenommen. Vom Landeskriminalamt habe ich mir hierzu **Ausdrucke der Protokolldaten** der ersten 1.000 Abfragen eines aktuellen Datums der Dateien
- Informationssystem Bayerische Polizei (IBP)
- Zentrales Verkehrsinformationssystem (ZEVIS)
- Einwohnermeldeamtsverfahren (EWO)
- Ausländerzentralregister (AZR)

fertigen lassen.

Aus den protokollierten Abfragen habe ich stichprobenartig einzelne Datensätze an das Polizeipräsidium Oberfranken mit der Bitte weitergegeben, die mit Hilfe der individuellen Stammnummer identifizierten Polizeibeamten **nach dem Grund der Abfrage in der Datei zu befragen.** Die Befragung sollte klären, ob die gesetzlichen Voraussetzungen für die Dateiabfrage vorgelegen haben, und der jeweilige Polizeibeamte die Daten zur Erfüllung **polizeilicher** Aufgaben verwendet hat.

Bei der Auswertung der Protokollierung konnte zunächst für einzelne Abfragen keine befriedigende Erklärung gegeben werden. Mehrere Polizeibeamte gaben an, die unter ihrer Stammnummer aufgezeichneten Abfragen nicht durchgeführt zu haben. Dies konnte zum Teil mit Abwesenheit vom Dienst zum Zeitpunkt der Abfrage belegt werden. Ich bin der Sache nachgegangen und habe festgestellt, daß bei der Protokollierung von Abfragen beim Landeskriminalamt Fehler auftraten, so daß **den protokollierten Abfragen falsche Stammnummern zugeordnet wurden.** Dies führte dazu, daß bei einer Vielzahl von Systemanfragen nicht die richtigen Abfragenveranlasser in den Listenauswertungen nachgewiesen waren. Eine Überprüfung der Rechtmäßigkeit der Abfrage war deshalb nicht möglich. Das Landeskriminalamt wird dafür Sorge tragen, daß sich derartige Fehler nicht wiederholen.

Eine weitere Prüfung von Abfragen mit Hilfe der Protokolldatei im Bereich des Polizeipräsidiums Unterfranken hat keine Anhaltspunkte für einen Datenmißbrauch durch die abfragenden Dienstkräfte der Polizei ergeben.

4.7.2 Anlaßabhängige Auswertungen der Protokolldatei

Auf Routinekontrollen allein konnte ich mich im Berichtszeitraum allerdings nicht beschränken. In einigen Fällen war es erforderlich, Kontrollen durchzuführen, die von einem **konkreten Mißbrauchsverdacht** ausgelöst waren:

1. Ein Petent hatte den Verdacht geäußert, daß ein Kontrahent sich unbefugt Angaben über ihn betreffende Strafverfahren bei der Staatsanwaltschaft oder den Polizeibehörden beschafft habe, um diese gegen ihn zu verwenden. Er vermutete, daß Angehörige von Polizeibehörden oder der Staatsanwaltschaft diese Angaben an seinen Kontrahenten weitergegeben haben.

   Da der Verdacht wegen der vom Kontrahenten umfangreich aufgelisteten behördeninternen Erkenntnisse über Ermittlungsverfahren nicht unbegründet erschien, habe ich umfangreiche datenschutzrechtliche Ermittlungen bei der Staatsanwaltschaft, beim Landeskriminalamt und beim Polizeipräsidium eingeleitet. Die Auswertung der über Abfragen im polizeilichen Informationssystem beim Landeskriminalamt geführten Protokolldatei für den in Betracht kommenden Zeitraum ergab zwar, daß die Daten des Petenten in einer Vielzahl von Fällen von Polizeibeamten des Landeskriminalamtes und des Polizeipräsidiums abgefragt worden waren. Die anschließende Überprüfung der entsprechenden Dateiabfragen haben aber keine Anhaltspunkte für einen Verstoß

gegen datenschutzrechtliche Bestimmungen durch Bedienstete der Polizei erbracht. Auch der Verdacht gegen Angehörige der Staatsanwaltschaft hat sich nicht bestätigt. Es war nicht auszuschließen, daß sich der Kontrahent des Petenten die Informationen auf legalem Weg verschafft hat.

2. Den bereits in meinem 14. Tätigkeitsbericht geschilderten Fall eines ehemaligen Parteifunktionärs, der als Polizeibeamter in Verdacht geriet, nach parteiinternen Auseinandersetzungen verschiedene polizeiliche Auskunftssysteme nach Speicherungen über seine parteiinternen Kontrahenten ohne dienstliche Veranlassung abgefragt zu haben, habe ich im Hinblick auf das in dieser Sache anhängige Strafverfahren noch nicht abgeschlossen. Die Auswertung der Protokolldatei hatte ergeben, daß unter der persönlichen Kennung des Polizeibeamten Personen im Kriminalaktennachweis sowie im polizeilichen Fahndungsbestand abgefragt worden waren. Nachdem das Strafverfahren nunmehr wegen der Rücknahme des Strafantrags durch den Verletzten gemäß § 206a StPO eingestellt wurde, habe ich meine Ermittlungen wieder aufgenommen.

4.8 Anwendung des Polizeiaufgabengesetzes (PAG)

4.8.1 Mitteilung des Verfahrensausgangs durch die Staatsanwaltschaft an die Polizei

Der **Ausgang des Ermittlungsverfahrens** bei der Justiz ist für die weitere Speicherung von personenbezogenen Daten im Kriminalaktennachweis und für die weitere Aufbewahrung der Kriminalakte von **erheblicher Bedeutung.** Angesichts der Entscheidung der Justiz muß sich die Polizei fragen, ob ihr **Verdacht noch berechtigt** und die weitere Speicherung zulässig ist.

Wie ich bereits im 14. Tätigkeitsbericht berichtet habe, hat das Innenministerium in Absprache mit dem Justizministerium eine Dienstanweisung erlassen, nach der die Polizei eine **Einzelfallprüfung** der Notwendigkeit der weiteren Speicherung stets vorzunehmen hat, wenn

- nach der Beurteilung der Justiz jeglicher **Tatverdacht entfallen** ist, und dies dem Beschuldigten **mitgeteilt** wurde
- die Strafbarkeit der Tat wegen Änderung des Strafrechts entfallen ist oder
- der Angeklagte freigesprochen wurde.

Durch die Dienstanweisung ist gewährleistet, daß die Polizei die Informationen erhält, die sie für ihre Entscheidung über den Wegfall des Tatverdachts (Art. 38 Abs. 2 PAG) benötigt. Dies gilt im Fall der Einstellung des Verfahrens, wenn der **Beschuldigte als solcher vernommen** worden ist oder ein Haftbefehl gegen ihn erlassen worden war oder wenn er um einen **Bescheid gebeten** hat oder ein **besonderes Interesse** an der Bekanntgabe ersichtlich ist (§ 170 Abs. 2 Satz 2 StPO).

Wie mir das Innenministerium auf Anfrage mitgeteilt hat, dürften damit Fälle, in denen die Polizei vom Wegfall des Tatverdachts nicht unterrichtet wird, in der Praxis kaum vorkommen. Ich werde diese Frage bei Kontrollen der Staatsanwaltschaften besonders im Auge behalten.

4.8.2 Datenübermittlung innerhalb des öffentlichen Bereichs

Erforderlichkeit

Im täglichen Verwaltungsvollzug kommt es in einer Vielzahl von Fällen zu Übermittlungen personenbezogener Daten von Polizeibehörden an andere öffentliche Stellen. So bitten beispielsweise regelmäßig die Kreisverwaltungsbehörden um Übermittlung von polizeilichen Erkenntnissen, um vor Erteilung eines Waffenscheins, einer Gaststättenerlaubnis o.ä. die Zuverlässigkeit des Antragstellers zu überprüfen.

Auf Ersuchen von Behörden und öffentlichen Stellen kann die Polizei personenbezogene Daten übermitteln, soweit dies

- zur Wahrnehmung von Aufgaben der Gefahrenabwehr durch den Empfänger,
- zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
- zur Wahrung sonstiger schutzwürdiger Interessen

erforderlich ist.

Deshalb darf die Polizei bei einer allgemein gehaltenen Anfrage nach „Erkenntnissen" nicht wahllos jedes von ihr in den verschiedenen polizeilichen Dateien und Akten gespeicherte Datum übermitteln. Vielmehr hat sie vor der Datenübermittlung eine **Auswahl unter dem Gesichtspunkt der Erforderlichkeit** der Daten für die Aufgabenerfüllung durch die anfragende Behörde zu treffen. So ist beispielsweise die Kenntnis einer bei der Polizei zu einer Person gespeicherten Beleidigung zwischen Nachbarn oder zu einer geringfügigen Ordnungswidrigkeit nicht in jedem Fall zur Aufgabenerfüllung durch die anfragende Behörde erforderlich.

Dokumentation

Wie die Polizei in der **Praxis** verfährt, insbesondere ob und wie sie bei der Beantwortung der Anfrage eine Auswahl trifft, konnte ich bei der Prüfung einer Polizeidirektion **nicht feststellen,** da die Anfragen der ersuchenden Behörden nach Beantwortung jeweils urschriftlich dorthin zurückgesandt wurden, ohne daß darüber Unterlagen oder Nachweise bei der Polizei geführt werden. Ich habe deshalb eine **Dokumentation der Anfragen** und Antworten für notwendig gehalten. Diese ist auch aus einem weiteren Grund erforderlich:
Erweisen sich einmal weitergegebene Daten nachträglich als unrichtig, so ist die Polizei nach dem Polizeiaufgabengesetz verpflichtet, die Daten unverzüglich gegenüber dem Empfänger zu **berichtigen,** wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist. Verzichtet die Polizei jedoch auf eine Dokumentation der Weitergabe von Informationen, so ist

eine nachträgliche Berichtigung nicht mehr möglich, da die Polizei nicht nachvollziehen kann, ob und welche Daten an welche Behörde übermittelt wurden.

Nach dem Entwurf der **Richtlinien für die Führung polizeilicher personenbezogener Sammlungen** ist in Zukunft von der Polizei festzuhalten, an wen Erkenntnisse weitergegeben wurden, wenn Auskünfte aus polizeilichen personenbezogenen Sammlungen an Berechtigte außerhalb der aktenführenden Dienststelle erteilt wurden. Soweit nichts Abweichendes in der Akte vermerkt wird, gilt der zu diesem Zeitpunkt bestehende Umfang an Sachverhalten als übermittelt. Diese Neuerung ist zu begrüßen.

Vollständigkeit von Auskünften

In einer Vielzahl von Fällen übermittelt die Polizei personenbezogene Daten aus Verfahren, die mittlerweile **eingestellt** wurden oder deren **Verfahrensausgang** der Polizei **unbekannt** ist. Die Übermittlung dieser Daten halte ich – soweit die sonstigen Voraussetzungen vorliegen – für zulässig, sofern die Polizei die anfragende Behörde auf die Einstellung des Verfahrens oder auf den ihr unbekannten Verfahrensausgang ausdrücklich **hinweist.** Es ist Sache der anfragenden Behörde, die Gründe für die Einstellung oder den Ausgang des Verfahrens festzustellen, wenn dies für ihre Aufgabenerfüllung von Bedeutung ist.

Keine Bindung durch Bundeszentralregister

Die Polizei kann auch über Speicherungen verfügen, die **im Bundeszentralregister bereits gelöscht** sind. Grund dafür sind die unterschiedlichen Speicherungsfristen bei Polizei und registerführender Behörde.

Im Bundeszentralregister getilgte Eintragungen dürfen nach dem Bundeszentralregistergesetz (BZRG) dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden. Regelmäßig wird die Polizei gar nicht wissen, ob die Eintragungen bereits getilgt sind. Sie ist auch nicht verpflichtet, dies durch Einholung einer Auskunft aus dem Bundeszentralregister vor der Datenübermittlung festzustellen, da auch die Übermittlung von Speicherungen der Polizei, die sich auf getilgte Eintragungen beziehen, zulässig ist. Es handelt sich dabei um einen internen Vorgang zwischen Behörden, der vom BZRG nicht erfaßt wird. **Erst die anfragende Behörde,** die die ihr übermittelten Erkenntnisse gegenüber dem Betroffenen verwenden will, muß dabei die vom BZRG gesetzten Grenzen beachten.

4.8.3 Mitteilung von Rahmenerrichtungsanordnungen

Nach Art. 47 Abs. 1 Polizeiaufgabengesetz sind für den erstmaligen Einsatz von automatisierten Verfahren bei der Polizei, mit denen personenbezogene Daten verarbeitet werden, in einer Errichtungsanordnung die dort unter Nr. 1–10 aufgeführten Punkte (speichernde Stelle, Bezeichnung der Datei, Zweck der Datei, betroffener Personenkreis, Art der zu speichernden Daten, Eingabeberechtigung, Zugangsberechtigung, regelmäßige Datenübermittlungen, Überprüfungsfristen, Speicherungsdauer sowie Protokollierung des Abrufs) festzulegen. Nach der Zustimmung des Innenministeriums ist die Errichtungsanordnung dem Landesbeauftragten für den Datenschutz mitzuteilen. Diese Mitteilungen dienen sowohl meiner Information über die Datenverarbeitung bei der Polizei als auch der Kontrolle der datenschutzrechtlichen Zulässigkeit der gewählten Verfahren.

Diesen Zweck kann die Mitteilung nur erfüllen, wenn sie **hinreichend konkret** ist und die Angaben insbesondere zum **Zweck** der Datei, zum betroffenen **Personenkreis** und zur **Art** der zu speichernden Daten eine Beurteilung aus datenschutzrechtlicher Sicht zulassen. Diesem Anspruch werden **Rahmen**errichtungsanordnungen nicht gerecht. Dies zeigt sich in besonderem Maße am Beispiel der Rahmenerrichtungsanordnung für die Dateien „Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten" (GAST-Dateien). Unter dieser Verfahrensbezeichnung werden ganz unterschiedliche Dateien (z.B. Prostituiertendatei, Gaststättendatei, Fahrraddatei) betrieben, an die aus datenschutzrechtlicher Sicht unterschiedliche Maßstäbe anzulegen sind.

Das Innenministerium hat die Errichtungsanordnung „GAST" überarbeitet und dabei folgende Ergänzungen aufgenommen:

1. „GAST"-Dateien sind in das Verzeichnis freigegebener automatisierter Verfahren der Präsidien aufzunehmen.
2. Die Genehmigung zur Einrichtung von GAST-Dateien im Einzelfall wird den Polizeipräsidien übertragen. Die vorliegende Errichtungsanordnung legt den maximalen Rahmen von Datenspeicherungen fest, so daß entsprechend dem Dateizweck Beschränkungen geboten sein können (z.B. betroffener Personenkreis, Umfang, Prüfungsfristen zur Löschung). Solche Beschränkungen sind im Genehmigungsschreiben anzugeben, ggf. ist eine eigene Errichtungsanordnung zu erstellen. Die erforderlichen Fristen, nach der die speichernde Stelle in angemessenem Abstand die Notwendigkeit der Weiterführung oder Änderung ihrer Datei zu überprüfen hat (Art. 47 Abs. 2 Polizeiaufgabengesetz), sind festzulegen. Ein Abdruck der Genehmigung ist dem Landesbeauftragten für den Datenschutz zuzuleiten.

Abgesehen von dem unter Nr. 1 genannten Verzeichnis, das mir auf Anforderung zuzuleiten ist, werde ich danach in Zukunft durch Übersendung des Abdrucks neu genehmigter GAST-Dateien **aktuell unterrichtet.** Da die Genehmigung des Polizeipräsidiums hinreichend präzisiert sein muß, genügt dieses Verfahren meinem Informationsinteresse.

4.8.4 Auswertung von Protokollbeständen zur Kriminalitätsbekämpfung

Protokollbestände, die bei automatisierten Abfragen in polizeilichen Auskunftssystemen beim Landeskriminal-

amt entstehen, dienen in erster Linie der Datensicherung und damit auch meinen datenschutzrechtlichen Kontrollen, die ich aus besonderem Anlaß oder anlaßunabhängig mehrmals jährlich durchführe. Das Polizeiaufgabengesetz (Art. 46 Abs. 3 PAG) läßt daneben **die Auswertung von Protokollbeständen auch zu Zwecken der Kriminalitätsbekämpfung** zu. Sie bedarf einer Anordnung der in Art. 33 Abs. 5 PAG genannten Dienststellenleiter (Polizeipräsident, Direktionsleiter, LKA-Präsident).

Wie mir das Landeskriminalamt mitteilte, wurden im Zeitraum vom 1. Oktober 1992 bis 1. März 1993 insgesamt 58 Auswertungen der Protokolldatei zu Zwecken der Kriminalitätsbekämpfung vorgenommen. Davon erbrachten 16 Auswertungen kein Ergebnis. Von den verbleibenden 42 Auswertungen trugen nach Auskunft der einzelnen Dienststellen **32 Auswertungsergebnisse zur Fallklärung bei.**

Das Ergebnis zeigt, daß Forderungen nach einer engen Zweckbindung von Protokollbeständen, nämlich allein zur Datensicherung, nicht vertretbar sind.

4.9 Richtlinien für die Führung personenbezogener polizeilicher Sammlungen (PpS-Richtlinien)

Zur Erfüllung der polizeilichen Aufgaben werden bei den Behörden und Dienststellen der bayerischen Polizei **personenbezogene Sammlungen** (PpS) geführt, die alle erforderlichen Unterlagen enthalten, die im Zusammenhang mit der Aufgabenwahrnehmung der Polizei anfallen. Bei den polizeilichen personenbezogenen Sammlungen handelt es sich um **Vorgangssammlungen** (zur Dokumentation polizeilichen Handelns, zur Verwaltung der Vorgänge u.ä.) und um **kriminalpolizeiliche Sammlungen** (z.B. Kriminalakten, Fallakten, Meldedienstsammlungen).

Rechtsgrundlage für die Führung polizeilicher personenbezogener Sammlungen sind die Art. 37 ff. des Bayerischen Polizeiaufgabengesetzes (PAG). Nach Art. 38 Abs. 1 PAG kann die Polizei personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Die Polizei kann insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtigt sind, eine Straftat begangen zu haben, speichern, verändern und nutzen, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist (Art. 38 Abs. 2 Satz 1 PAG).

Aufgabe des vom Innenministerium vorgelegten Entwurfs der PpS-Richtlinien, der die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) aus dem Jahre 1981 ersetzen soll, ist es, – auf der Grundlage der gesetzlichen Vorgabe – **den Rahmen der polizeilichen Datenverarbeitung umfassend zu regeln.** Den Richtlinien kommt deshalb eine zentrale Bedeutung für den Umgang der Polizei mit personenbezogenen Daten der Bürger zu.

In einem Arbeitspapier habe ich mich gegenüber dem Innenministerium zu dem Entwurf geäußert und in einem Gespräch in einer Reihe von Punkten datenschutzrechtliche Verbesserungen erreichen können. Wichtige Forderungen habe ich bereits in meinem 14. Tätigkeitsbericht angesprochen:

1. **Reduzierung der im KAN zu speichernden Vorgänge**

   Der Entwurf sah bereits vor, daß **keine Kriminalakte geführt** wird wegen Straftaten nach § 218 Abs. 1 und 3 StGB (Schwangerschaftsabbruch durch die Schwangere), Verkehrsordnungswidrigkeiten sowie wegen sonstiger Ordnungswidrigkeiten und verkehrsrechtlicher Verstöße, die einen Straftatbestand erfüllen (sofern keine Anhaltspunkte dafür vorliegen, daß die Aufnahme zur Erfüllung auf dem Gebiet der Strafverfolgung oder der Gefahrenabwehr erforderlich ist).

   Darüber hinaus habe ich gefordert, zur Entschlackung des KAN auch nachfolgende Delikte künftig nicht mehr in die Datei aufzunehmen:

   - **Privatklagedelikte,** soweit von der Staatsanwaltschaft das öffentliche Interesse an der Anklageerhebung verneint wird,
   - **alle Fahrlässigkeitsdelikte.**

   Das Innenministerium hält die **Anlegung einer Kriminalakte bei Privatklagedelikten,** bei denen die Staatsanwaltschaft das öffentliche Interesse an der Anklageerhebung verneint hat, und die **Speicherung dieser Delikte im Kriminalaktennachweis** für erforderlich. Die Entscheidung der Staatsanwaltschaft über das Vorliegen eines „öffentlichen Interesses" stütze sich nicht auf Gesichtspunkte der Gefahrenabwehr, sondern stelle auf die Notwendigkeit der öffentlichen Strafverfolgung ab. Es könne daher nicht generell bei diesen Delikten von einer Speicherung abgesehen werden. Hingegen hat das Innenministerium Fahrlässigkeitsdelikte, die **nur auf Antrag** verfolgt werden, von der Speicherung im KAN ausgenommen. Bei den übrigen Fahrlässigkeitsdelikten hält es jedoch die Speicherung in der Kriminalakte für notwendig, da sich hinter manchen Fahrlässigkeitsdelikten vorsätzliche Delikte verbergen würden (z.B. bei fahrlässiger Brandstiftung). Die Praxis habe gezeigt, daß **Fahndungsansätze auch aus Fahrlässigkeitsdelikten** gewonnen werden können.

   Damit ist das Innenministerium meinen datenschutzrechtlichen Forderungen zum Teil nachgekommen. Im Hinblick auf die Erfahrungen der Praxis sehe ich vorerst von der Verfolgung meiner weitergehenden Forderungen ab. Bei künftigen KAN-Prüfungen werde ich auf die Privatklage- und Fahrlässigkeitsdelikte ein besonderes Auge werfen.

2. **Kürzung der Aussonderungsprüffrist**

Nach Art. 37 Abs. 3 PAG ist die Dauer der Speicherung polizeilicher personenbezogener Daten auf das erforderliche Maß zu beschränken. Es sind Termine festzulegen, an denen spätestens überprüft werden muß, ob die Speicherung von Daten weiterhin erforderlich ist. Diese festzulegenden Prüfungstermine oder Aufbewahrungsfristen dürfen nach Art. 38 Abs. 2 Satz 3 und 4 PAG bei Erwachsenen 10 Jahre, bei Jugendlichen 5 Jahre und bei Kindern 2 Jahre nicht überschreiten. In Fällen von **geringerer Bedeutung sind kürzere Fristen** festzusetzen.

Ich hatte bereits früher gefordert, Fallgruppen zu bilden, die in der Regel als solche von geringerer Bedeutung anzusehen seien (vgl. auch 14. Tätigkeitsbericht, Ziff. 4.8.2). Diese Forderung hat das Innenministerium aufgegriffen. Ein Fall geringerer Bedeutung wird nunmehr angenommen bei Fahrlässigkeitstaten, Beleidigungsdelikten, Hausfriedensbruch und vorsätzlicher Körperverletzung, soweit diese nicht in der Öffentlichkeit begangen wurden und die Staatsanwaltschaft das öffentliche Interesse an der Verfolgung der Tat nicht bejaht hat, sowie bei Ordnungswidrigkeiten.

Mit dem Innenministerium habe ich die Frage erörtert, ob der Katalog der Straftaten, bei denen ein Fall geringerer Bedeutung angenommen wird, noch **erweitert** werden kann. Ich habe die Auffassung vertreten, daß für Fälle der Beförderungserschleichung und des Diebstahls geringwertiger Sachen wegen des geringen Unrechtsgehalts – jedenfalls beim Ersttäter – eine kürzere Speicherungsfrist vorgesehen werden sollte. Dieser Auffassung konnte sich das Innenministerium jedoch nicht anschließen.

Da auch nach den Richtlinien **im Einzelfall weitere Straftaten als Fälle geringerer Bedeutung** in Betracht kommen, werde ich bei meinen **Prüfungen** verstärkt darauf achten, ob in geeigneten Fällen eine Fristverkürzung vorgenommen wurde. Möglicherweise lassen sich nach weiteren Erfahrungen dennoch zusätzliche Delikte generell als solche geringerer Bedeutung einstufen.

3. **Einschränkung der Fristverlängerungsautomatik bei Vermißtenfällen oder Suizidversuchen**

Nach Art. 38 Abs. 2 Satz 5 Polizeiaufgabengesetz beginnt die Aussonderungsprüffrist, nach deren Ablauf spätestens die Erforderlichkeit der weiteren Speicherung überprüft werden muß, regelmäßig mit dem Ende des Jahres, in dem das letzte Ereignis zu einer Person erfaßt worden ist. Deshalb kann sich die Speicherungsdauer bereits gespeicherter Ereignisse bei Zuspeicherung eines weiteren Vorfalles verlängern.

Ich hatte bereits früher vorgeschlagen, daß zumindest bei einer **Zuspeicherung von Vermißtenfällen oder Suizidversuchen von einer Verlängerung der Speicherungsdauer bereits gespeicherter Erkenntnisse abgesehen** wird (vgl. dazu 14. Tätigkeitsbericht, Ziff. 4.8.3).

Das Innenministerium ist auch mit dem neuen Richtlinienentwurf meinem Vorschlag nicht gefolgt. In meinem Gespräch habe ich nochmals auf die Problematik hingewiesen, daß eine im Kriminalaktennachweis gespeicherte Straftat, die kurz vor der Löschung steht, nur deswegen um weitere 5 Jahre gespeichert wird, weil der Betroffene zwischenzeitlich vermißt war oder einen Selbsttötungsversuch unternommen hat. Ich habe um nochmalige Überprüfung der Notwendigkeit dieser Fristverlängerungsautomatik gebeten. Eine Antwort des Innenministeriums steht noch aus.

4. **Berücksichtigung des Verfahrensausgangs bei der Speicherung von Straftaten und Ordnungswidrigkeiten**

Nach Art. 38 Abs. 2 Satz 2 Polizeiaufgabengesetz sind die von der Polizei gespeicherten personenbezogenen Daten zu löschen, wenn der der Speicherung zugrundeliegende Verdacht entfallen ist. Ich habe daher schon in der Vergangenheit darauf gedrungen, daß die Polizei in diesem Fall von der Staatsanwaltschaft über den Ausgang des Verfahrens und die dafür maßgebende Beurteilung der Justiz unterrichtet werden muß.

Wie ich bereits berichtet habe (vgl. 14. Tätigkeitsbericht, Ziff. 4.13), wird nunmehr durch eine **Dienstanweisung** sichergestellt, daß die Polizei die Informationen, die sie für ihre Entscheidung über den Wegfall des Tatverdachts benötigt, von der Staatsanwaltschaft erhält. Dies gilt auch bei Einstellungen des Ermittlungsverfahrens nach § 170 Abs. 2 StPO, sofern sich für die Justiz die Unschuld des Beschuldigten ergeben hat oder jeglicher begründeter Verdacht entfallen ist und dies dem Beschuldigten mitgeteilt wurde.

Diese Regelung hat Eingang in den Entwurf der PpS-Richtlinien gefunden.

Ich habe weiterhin gefordert, daß auch bei **Ordnungswidrigkeitenverfahren** von der Verfolgungsbehörde eine Mitteilung an die Polizei erfolgen muß, wenn sich die Unschuld des Betroffenen ergeben hat oder jeder begründete Verdacht entfallen ist.

Das Innenministerium hat diesen Vorschlag in seinem Entwurf insoweit berücksichtigt, als bei den Ordnungswidrigkeiten, die im Landes-Kriminalaktennachweis eingetragen werden, die gleiche Regelung zu gelten hat wie bei Straftaten. D.h., daß in den Fällen, in denen das Ordnungswidrigkeitenverfahren eingestellt wird, weil sich die Unschuld des Betroffenen ergeben hat oder jeder begründete Verdacht entfallen ist, auch eine Mitteilung an die Polizei durch die Verfolgungsbehörde erfolgen wird.

4.10 Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung – Verbrechensbekämpfung (PSV)"

Während Speicherungen im Kriminalaktennachweis (KAN) allein dem Zweck der polizeilichen Gefahrenabwehr dienen, werden in der PSV Daten gleichzeitig für **mehrere Zwecke** gespeichert. Die PSV dient nicht nur der **Vorgangsverwaltung** und der **Dokumentation,** sondern auch der **Gefahrenabwehr** einschließlich der **vorbeugenden Verbrechensbekämpfung.** Die noch offenen datenschutzrechtlichen Fragen habe ich mit dem Innenministerium erörtert:

1. **Verlängerung der Aufbewahrungsfrist**

   Nach der Errichtungsanordnung für die Datei PSV kann der Sachbearbeiter durch Eintragen eines Termins die Speicherungsfrist für Strafanzeigen, die nicht in eine Kriminalakte aufgenommen wurden, **verlängern,** wenn im Einzelfall eine längere Aufbewahrungsfrist zum Zwecke der **Vorgangsverwaltung/Sachbearbeitung** geboten ist. Wird z.B. der Vorgang eines Kindes nach der in Art. 38 Abs. 2 Satz 3 PAG für tatverdächtige Kinder vorgesehenen Regelfrist von zwei Jahren nur deshalb nicht vernichtet, weil etwa noch zivilrechtliche Ansprüche zu klären sind und die Unterlagen dafür benötigt werden, so dürfen die personenbezogenen Daten des Kindes nur noch zu diesem Zweck (Vorgangsverwaltung, Dokumentation), nicht aber auch zum Zwecke der **vorbeugenden Verbrechensbekämpfung** gespeichert werden.

   Gleichwohl stehen die personenbezogenen Daten des betroffenen Kindes für die Dauer der Speicherung weiter auch für die Kriminalitätsbekämpfung zur Verfügung. Die vorgesehene weitere Speicherung des Kindes als Beschuldigter auch für diesen Zweck halte ich nicht für zulässig. Gleiches gilt – mit anderen Fristen (5 Jahre) – wenn nicht ein Kind, sondern ein Erwachsener von der Verlängerung der Speicherung betroffen ist. Ich habe deshalb eine Beschränkung des Speicherungszwecks und der Zugriffsberechtigung auf eine nicht mit der unmittelbaren Kriminalitätsbekämpfung befaßte Stelle gefordert.

   Das Innenministerium hat meine Forderung aufgegriffen und wird künftig, sofern keine Verlängerungsgründe nach Art. 38 Abs. 3 PAG gegeben sind, die Personalien des Kindes nach 2 Jahren mit einem **Satzschutz** belegen lassen. Die Vergabe der Zugriffsberechtigung auf die Personendaten des Kindes für Zwecke der **Vorgangsverwaltung** wird den Behördenleitern übertragen, wobei die zu berechtigende Stelle nicht mit der unmittelbaren Kriminalitätsbekämpfung befaßt sein darf (z.B. Systemverwalter einer Dienststelle).

   Eine entsprechende Regelung ist auch für die Verlängerung der Speicherung personenbezogener Daten Erwachsener vorzusehen.

2. **Wegfall des Tatverdachts**

   Nach der Dienstanweisung PSV ist die weitere Speicherung einer zunächst in der Eigenschaft als Tatverdächtiger/Betroffener gespeicherten Person auch nach Wegfall dieser Eigenschaft zulässig, wenn dies für Zwecke der **Vorgangsverwaltung/Sachbearbeitung** weiterhin erforderlich erscheint. Aus der weiteren Speicherung der Person darf sich jedoch die bisherige, weggefallene Eigenschaft nicht mehr ergeben.

   Beim Polizeipräsidium München werden die sog. B-Personalien (Beschuldigter/Betroffener) nach Wegfall des Tatverdachts aufgrund Sachbearbeiterentscheidung in „Z-Personalien" (Zeuge) geändert. Zusätzlich erhalten die Z-Personalien den Datenfeldzusatz „E" (Ermittlungsdaten). Darüber hinaus kann ein Sondervermerk im System gespeichert werden, aus dem hervorgeht, daß der Tatverdacht gegen den von der Speicherung Betroffenen entfallen ist. Der Name des Betroffenen ist von **allen** Beamten abrufbar.

   Das Innenministerium hat veranlaßt, daß die Bayer. Polizei künftig einheitlich das beim Polizeipräsidium München angewendete Verfahren zu vollziehen hat. Dieses Verfahren halte ich für vertretbar, da es zwar nicht zu einer Löschung der gespeicherten Personendaten, wohl aber zu einer Löschung im Datenblock „Beschuldigter" (B) führt. Die Eintragung seiner Personendaten in den Datenblock des Zeugen (Z) ist erforderlich, da bei einem notwendigen Rückgriff auf den Vorgang eine personenbezogene Suche möglich sein muß.

3. **Fehlende Protokollierung**

   Die aus der Sicht des Datenschutzes erforderliche Protokollierung von Abfragen in der Datei PSV findet derzeit nicht statt. Sie ist wegen der umfangreichen Zugriffsmöglichkeiten aus prophylaktischen Gründen, aber auch zur effektiven Datenschutzkontrolle aus meiner Sicht **unverzichtbar. Es ist deshalb dringend notwendig, daß die technischen Voraussetzungen für eine Protokollierung mit Nachdruck geschaffen werden und die Protokollierung realisiert wird.**

   Das Innenministerium steht meiner Forderung aufgeschlossen gegenüber. Es weist aber darauf hin, daß die Protokollierung zum gegenwärtigen Zeitpunkt aus technischen und haushaltsmäßigen Sachzwängen vorerst nicht durchgeführt werden kann. Diese Verfahrensweise sei auch vertretbar, weil die Protokollierung nur dann als erforderlich betrachtet werden müsse, wenn ihre Einführung und der damit verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehe (Art. 15 Abs. 1 BayDSG). Da die Datei PSV zum gegenwärtigen Zeitpunkt nur auf örtlicher Ebene betrieben werden könne (sog. Insellösung), beschränke sich der Aus-

kunftsumfang auf Inhalte der bisher in einer Polizeiinspektion geführten Tagebücher. Erst mit Einrichtung der 2. Ausbaustufe von IBP werde der inspektions-/direktionsübergreifende **Zugriff** (innerhalb eines Polizeipräsidiums) möglich sein. Wesentlich sei hierbei, daß solche Dialoge stets über den Rechner des Landeskriminalamts abgewickelt würden und das für Landesanwendungen (KAN, ZEVIS usw.) **bestehende Protokollierungsverfahren** dann entsprechend **übernommen werden könne.**

Das zeitlich befristete Fehlen einer Protokollierung von Abfragen in der PSV erscheint mir in Anbetracht dieser Umstände hinnehmbar.

4.11 Bundesweites Meldesystem „fremdenfeindliche Straftaten"

Fremdenfeindliche rechtsextremistisch motivierte Straftaten haben einen besorgniserregenden Umfang angenommen. Die Innenministerkonferenz hat sich deshalb auf folgende datenschutzrechtlich relevanten polizeilichen Maßnahmen zur Bekämpfung dieser Straftaten geeinigt:

1. Die **Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen** werden um „fremdenfeindliche Straftaten" ergänzt. Als „fremdenfeindlich" wird eine Straftat angesehen,
   - die in der Zielrichtung gegen Personen begangen wird, denen die Täter (aus intoleranter Haltung heraus) aufgrund ihrer tatsächlichen oder vermeintlichen Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe, Religion, Weltanschauung, Herkunft oder aufgrund ihres äußeren Erscheinungsbildes ein Bleibe- oder Aufenthaltsrecht in der Wohnumgebung oder in der gesamten Bundesrepublik bestreiten oder
   - die gegen sonstige Personen/Institutionen/Objekte/ Sachen begangen wird, bei denen die Täter aus fremdenfeindlichen Motiven heraus handeln.
2. Täter „fremdenfeindlicher Straftaten" können in Zukunft in der Arbeitsdatei PIOS-Innere Sicherheit **(APIS)** erfaßt werden.
3. Fremdenfeindliche Straftaten werden als überregional bedeutsam betrachtet und dementsprechend im **Bundes-KAN** erfaßt.
4. Die Errichtungsanordnungen für die Dateien „Personenfahndung", „Kriminalaktennachweis" und „Erkennungsdienst" werden jeweils um den **personengebundenen Hinweis „fremdenfeindlich"** ergänzt. Dieser personengebundene Hinweis darf nur vergeben werden, wenn Anhaltspunkte dafür vorliegen, daß die tatverdächtige Person Straftaten gegen Personen oder Sachen aus fremdenfeindlichen Beweggründen begangen hat.

Gegen die Definition der „fremdenfeindlichen Straftat" besteht aus meiner Sicht keine Bedenken. Sie berücksichtigt das Persönlichkeitsrecht des einzelnen und das aus Gründen der öffentlichen Sicherheit und Ordnung notwendige Informationsinteresse der Polizei in angemessener Weise.

Auch die vorgesehenen erweiterten Speicherungsmöglichkeiten halte ich aus datenschutzrechtlicher Sicht für unbedenklich. Zweck des Meldedienstes und der Speicherung in APIS ist es unter anderem, durch Sammlung und Auswertung von Nachrichten und Unterlagen Hinweise für die Verhütung und Aufklärung von Straftaten zu gewinnen, die sich gegen die freiheitliche demokratische Grundordnung richten. Zu ihren grundlegenden Prinzipien gehört auch die Achtung der Menschenwürde, das Recht der Persönlichkeit auf Leben und freie Entfaltung, somit auch der Schutz aller Menschen vor Straftaten, auch wenn sie anderer Herkunft, Rasse oder ähnliches sind. Die Qualifizierung der fremdenfeindlichen Straftat in obenbenanntem Sinn reicht deshalb stets zur Speicherung in APIS aus.

Ebenso ist die Erfassung von „fremdenfeindlichen Straftaten" im Bundes-KAN erforderlich und angemessen. Fremdenfeindliche Straftaten sind als überregional bedeutsam einzustufen. Die Ereignisse in der jüngsten Vergangenheit haben gezeigt, daß fremdenfeindliche Straftaten überregionalen Bezug haben. Die Möglichkeit, bundesweit von solchen Straftaten und Straftätern Kenntnis zu nehmen, ist für die Polizei erforderlich, um Entwicklungen zu erkennen, Gefahrenvorsorge zu betreiben und im konkreten Einzelfall aufgrund der vorliegenden Erkenntnis die gebotene Taktik und gefahrenabwehrende Maßnahmen ergreifen zu können. Eine Speicherung allein im APIS reicht nicht aus, da der polizeiliche Zugriff auf diese Datei stark beschränkt ist. Ich bin der Meinung, daß es nicht das Ziel des Datenschutzes sein kann, die Polizei durch zu hohe datenschutzrechtliche Anforderungen an der Beschaffung der Informationen zu hindern, die zur wirksamen Bekämpfung des Rechtsextremismus erforderlich sind.

4.12 Datei „Schleuser"

Schon lange haben die einschlägigen Kreise erkannt, daß mit der illegalen Einreise von Ausländern in die Bundesrepublik Deutschland ein „gutes Geschäft" zu machen ist. Einzelne Schleuser, aber auch ganze Schleuserorganisationen, haben sich dieses Marktes angenommen und bieten ihre Hilfe bei der Umgehung deutscher Einreisebestimmungen an.

Zur Bekämpfung der anwachsenden Schleuserkriminalität (§ 92 Abs. 2 Ausländergesetz) wurde am 1. Februar 1993 die Falldatei „Schleuser und Geschleuster" (FDS) geschaffen. Die FDS soll für ein Jahr **erprobt** werden. An der Erprobung nehmen neben Bayern die Länder Baden-Württemberg, Nordrhein-Westfalen und Sachsen teil.

Die FDS ist eine Verbunddatei, die beim Bundeskriminalamt betrieben wird. Sie dient der Aufklärung und Ver-

hütung von illegaler Schleusertätigkeit und damit zusammenhängenden Straftaten. In die FDS aufgenommen werden Daten von

- Beschuldigten im Rahmen eines strafrechtlichen Ermittlungsverfahrens und
- Verdächtigen (Personen, die nicht Beschuldigte sind, bei denen aber Anhaltspunkte dafür vorliegen, daß sie Täter oder Teilnehmer einer mit der illegalen Schleusertätigkeit zusammenhängenden Straftat sind).

Gegen die probeweise Einführung der Datei habe ich keine grundsätzlichen datenschutzrechtlichen Bedenken. Insbesondere halte ich neben der Erfassung von Schleusern auch die **Erfassung von Geschleusten** zur Bekämpfung von illegaler Schleusertätigkeit und damit zusammenhängender Straftaten und zur Verhinderung der illegalen Einreise und des illegalen Aufenthalts von Ausländern für erforderlich, weil durch die Speicherung Tatzusammenhänge und Täterverbindungen in diesem Bereich erkannt werden können. Der Kriminalaktennachweis (KAN) allein ist für dieses Informationsbedürfnis der Polizei nicht ausreichend. Zum einen ist der Zugriff der Polizei auf den eigenen Landesbestand beschränkt, zum anderen gibt der KAN keine Auskunft über den konkreten Sachverhalt, der sich hinter der Speicherung verbirgt.

Nach Ablauf der Erprobung wird zu prüfen sein, ob sich die in die Datei gesetzten Erwartungen erfüllt haben. Es geht aber nicht an, zur polizeilichen Aufgabenerfüllung geeignet und erforderlich erscheinende Maßnahmen von vornherein abzulehnen, weil der Nachweis ihrer Wirksamkeit noch nicht erbracht ist.

4.13 AFIS-Erfassungsstationen

1. Nach dem Asylverfahrensgesetz vom 30. Juni 1993 sind grundsätzlich **alle Asylbewerber erkennungsdienstlich zu behandeln,** damit Asylmißbrauch und Sozialbetrug wirksam bekämpft werden können. Zur erkennungsdienstlichen Behandlung gehört auch die Abnahme der **Fingerabdrücke,** die eine sichere Identifizierung des Betroffenen ermöglichen. Dazu werden die Fingerabdrücke bei der Polizei abgenommen, vom BKA verformelt, gespeichert und ggf. mit anderen Fingerabdrücken verglichen. Diese Arbeiten waren bisher mit erheblichem Zeitaufwand verbunden.

   Seit Dezember 1992 werden die Fingerabdrücke von Asylbewerbern durch das BKA mit dem Automatischen Fingerabdruck-Identifizierungssystem (AFIS) verarbeitet. Durch AFIS wurde die erkennungsdienstliche Arbeit erheblich erleichtert (z.B. schnelleres Einlesen, bessere Recherchemöglichkeiten).

2. Für die Zwecke der **Kriminalitätsbekämpfung** (Spurenvergleich) kann AFIS voraussichtlich ab Ende 1993 genutzt werden. Sobald bei den Landeskriminalämtern sog. Erfassungsstationen installiert sind, können zur Spurenverursacheridentifizierung Tatortspuren (Fingerabdrücke oder Fingerabdruckfragmente) automatisiert an das Bundeskriminalamt übermittelt werden. Dort werden die Tatortspuren mit den in der Datei AFIS vorhandenen Fingerabdrücken verglichen. „Treffer" werden dem polizeilichen Sachbearbeiter am Bildschirm aufgezeigt. Wird ein Spurenverursacher ermittelt, können seine Personalien anhand der daktyloskopischen Nummer des verarbeiteten Fingerabdrucks über die Datei INPOL festgestellt werden. Bis zur Feststellung des Spurenverursachers läuft der Spurenvergleich anonym, d.h. ohne die Verwendung von Personalien ab.

3. Ein Vergleich von **Tatortspuren mit Fingerabdrücken von Asylbewerbern** ist unter den Voraussetzungen des § 16 Abs. 5 Asylverfahrensgesetz zur Feststellung der Identität oder der Zuordnung von Beweismitteln zulässig, wenn bestimmte Tatsachen die Annahme begründen, daß dies zur Aufklärung einer Straftat führen wird oder wenn es zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist. Auf eine Dokumentation der Gründe für einen solchen Vergleich sollte jedoch Wert gelegt werden.

4. Bewertung

   Der Einsatz von AFIS-Erfassungsstationen zur Kriminalitätsbekämpfung, wie er im Landeskriminalamt derzeit vorbereitet wird, stellt nach meiner Beurteilung nur eine **technische Erleichterung** des bisher schon durchgeführten Tatortspur-Fingerabdruckvergleichs dar. Eine aus datenschutzrechtlicher Sicht qualitativ wesentliche Änderung durch den Einsatz der EDV in diesem Bereich sehe ich nicht. Grundsätzliche Bedenken gegen das Verfahren habe ich deshalb nicht erhoben.

4.14 Datenübermittlung im EU-Bereich

Die europäische Integration hat auch Auswirkungen auf die grenzüberschreitende informationelle Zusammenarbeit. Besonders in zwei Bereichen ist ein **intensiver Austausch** personenbezogener Daten vorgesehen. Da dieser auch Daten erfaßt, die von bayerischen Polizeidienststellen im INPOL-Bund gespeichert wurden, sind auch bayerische datenschutzrechtliche Interessen berührt.

1. **EUROPOL-Drogenzentralstelle (EDU)**

   Das angestrebte Ziel einer institutionalisierten polizeilichen Zusammenarbeit auf europäischer Ebene ist die Schaffung einer europäischen Zentralstelle (EUROPOL). Als ersten Schritt auf diesem Weg soll im **Drogenbereich** die Möglichkeit des Informationsaustausches geschaffen werden. Dazu dient die Einrichtung eines Kooperationsstabes EDU (European Drug Unit). Geplant ist zunächst die Entsendung eines oder mehrerer Verbindungsbeamter durch jeden Mitgliedsstaat. Diese Verbindungsbeamten erhalten Zugriff nur zu ihren jeweiligen nationalen In-

formationssystemen. Der Kooperationsstab ist **nicht berechtigt, eine eigene Datei** mit personenbezogenen Daten zu führen. Eine besondere **Rechtsgrundlage** für diese Zusammenarbeit gibt es bisher noch nicht. Bis zur Schaffung einer solchen Rechtsgrundlage stützt sich die Zusammenarbeit auf eine **Vereinbarung** der zuständigen Minister und die Übermittlung der von den Polizeibehörden der Bundesländer gespeicherten Daten auf die jeweiligen **Landespolizeigesetze,** wie z.B. das Bayerische Polizeiaufgabengesetz (Art. 40 Abs. 5).

Nach meiner Auffassung liegt es grundsätzlich in der Zuständigkeit der **Bundesländer,** über die Übermittlung von Daten, die sie an das Bundeskriminalamt weitergegeben haben, an die Verbindungsbeamten der anderen Unionsländer zu entscheiden. Der Verbindungsbeamte des BKA, der Zugriff auf dort geführte INPOL-Dateien erhält, muß also vor einer Übermittlung von „Länderdaten" das **Einverständnis des jeweiligen Bundeslandes einholen,** das die Zulässigkeit nach Landesrecht prüft. Diese Beurteilung wird auch vom Bayerischen Innenministerium geteilt.

2. **Das Schengener Informationssystem (SIS):**

Das Schengener Übereinkommen vom 19. Juni 1990 regelt die vollständige Aufhebung aller Personenkontrollen an den Binnengrenzen der Vertragsstaaten sowie Ausgleichsmaßnahmen, um Sicherheitseinbußen, die durch den Verzicht auf Grenzkontrollen entstehen können, zu vermeiden. Eine der Ausgleichsmaßnahmen ist das **Schengener Informationssystem (SIS).** In das SIS sollen **alle Ausschreibungen, die der Suche nach Personen und Sachen dienen,** für polizeiliche Kontrollen und Überprüfungen an den Außengrenzen und im Landesinneren zum Abruf im automatisierten Verfahren eingegeben werden. In den nationalen Teil von SIS werden auch vom Bayerischen Landeskriminalamt personenbezogene Daten eingestellt werden. Die Zulässigkeit der Weitergabe dieser Daten wird von mir – wie bereits bisher die Weitergabe an die Verbunddateien „Fahndung" beim Bundeskriminalamt – überprüft. Jede Vertragspartei wird eine **nationale Kontrollinstanz** bezeichnen, deren Aufgabe darin besteht, nach Maßgabe des jeweiligen nationalen Rechts den Bestand des nationalen Teils des SIS unabhängig zu überwachen und zu prüfen, ob durch Verarbeitung und Nutzung der in SIS gespeicherten Daten die Rechte des Betroffenen nicht verletzt werden. Zur **Überwachung der technischen Unterstützungseinheit des SIS** wird eine **gemeinsame Kontrollinstanz eingerichtet, die sich aus je zwei Vertretern der jeweiligen nationalen Kontrollinstanzen zusammensetzt** (derzeit 18 Personen). Diese vielköpfige supranationale Kontrollinstanz soll mindestens zweimal jährlich den in Straßburg installierten Computer überprüfen.

4.15 Bürgereingaben

Im Berichtszeitraum wandten sich wieder Bürger an mich, die befürchteten, die Polizei habe in rechtlich unzulässiger Weise ihre personenbezogenen Daten erhoben, verarbeitet oder genutzt.

Meine Kontrollen haben ergeben, daß in den **meisten Fällen Beanstandungen nicht veranlaßt waren.** Lediglich in Einzelfällen habe ich die Verkürzung von Speicherfristen und die Löschung von Daten einschließlich der Vernichtung polizeilicher Unterlagen durch die Polizei verlangt sowie die Weitergabe von Daten gerügt. Folgende Fälle erscheinen mir berichtenswert:

1. **„Politisch motivierter Täter"**

Ein Petent erfuhr im Rahmen eines Ermittlungsverfahrens, in dem er Anzeigeerstatter war, daß er wegen mehrerer Straftaten bei der Polizei gespeichert war und dort als „politisch motivierter Täter" geführt wurde. Meine Überprüfung ergab, daß die Vergabe des personengebundenen Hinweises **„politisch motivierter Täter"** (POLT) durch die Polizei nicht gerechtfertigt war. Dieser Hinweis setzt den Verdacht einer Straftat voraus, bei der nach gesicherten Erkenntnissen anzunehmen ist, daß diese **zur Verfolgung politisch extremistischer Ziele begangen** wurde. Diese Voraussetzungen lagen nach dem Inhalt der polizeilichen Kriminalakte bei dem Petenten nicht vor. Es hatte sich lediglich um den Verdacht (unpolitischer) Straftaten gehandelt, die der Betroffene in seiner Eigenschaft als Funktionär einer Partei begangen haben soll, außerdem war die Vergabe des PHW „POLT" zum Zeitpunkt der Einspeicherung grundsätzlich nicht mehr zulässig. Ich habe daher gebeten, den personengebundenen Hinweis zu löschen. Diesem Wunsch hat die Polizei entsprochen.

Darüber hinaus ergaben meine Nachforschungen, daß die Ermittlungsverfahren, die zur Speicherung des Petenten im Kriminalaktennachweis der Polizei geführt hatten, von der Staatsanwaltschaft gemäß § 170 Abs. 2 Strafprozeßordnung eingestellt worden waren. Ich habe daraufhin die zuständige Polizeibehörde gebeten zu überprüfen, ob der für die weitere Speicherung erforderliche **Tatverdacht** fortbesteht. Die Polizeibehörde hat daraufhin die Speicherungen gelöscht und die dazu gehörenden Akten vernichtet.

2. **Polizeibericht im Bauakt**

Drei Personen, die eine Diskothek betreiben wollten, erfuhren, daß das Bauordnungsamt während des für die Eröffnung der Diskothek erforderlichen Genehmigungsverfahrens ein anonymes Schreiben, das baurechtliche und strafrechtliche Vorwürfe gegen sie enthielt, an die Polizei weitergegeben und die von der Polizei daraufhin übersandten personenbezogenen Erkenntnisse zum Bauakt genommen hatte. Diese seien dadurch dem Eigentümer der Räume, in dem

die Diskothek betrieben werden sollte, zur Kenntnis gelangt, als er in Vollmacht eines der Betroffenen in die Bauakte Einsicht nahm.

Meine Überprüfung des Vorganges ergab folgendes:

Das anonyme Schreiben war an den Oberbürgermeister der betreffenden Stadt gerichtet. Der Oberbürgermeister gab das anonyme Schreiben weiter an das **Bauordnungsamt** der Stadt. Dies war in entsprechender Anwendung des Art. 17 Abs. 1 und 3 BayDSG zulässig. Das Bauordnungsamt hatte zu prüfen, ob der Vorwurf fehlender Baugenehmigung zutreffend war und ggf. die entsprechenden Maßnahmen zu treffen.

Wegen der anonymen Hinweise auf Straftaten im Zusammenhang mit dem Betrieb anderweitiger von den Betroffenen geführten Diskotheken sandte das Bauordnungsamt das Schreiben an die örtliche **Kriminalpolizeiinspektion.** Dies war nach Art. 17 Abs. 1 Bayerisches Datenschutzgesetz ebenfalls zulässig, da die Übermittlung der personenbezogenen Daten an die Polizei zur Abwehr von Gefahren beim künftigen Betrieb der Diskothek durch die Polizei dienen konnte. Das Zuleitungsschreiben des Bauordnungsamtes war allerdings so unklar abgefaßt, daß die örtliche Polizei es als Ersuchen um Mitteilung von Erkenntnissen verstand.

Die örtliche Polizei wandte sich an das für die Betroffenen zuständige Polizeipräsidium mit der Bitte um Kenntnisnahme vom Inhalt des anonymen Schreibens und um Erkenntnismitteilung. Das Polizeipräsidium übermittelte daraufhin die bei ihm zu den im anonymen Schreiben genannten Personen vorhandenen Erkenntnisse aus der Datei Kriminalaktennachweis und den dazugehörenden Kriminalakten an die örtliche Polizei.

Die übermittelten Erkenntnisse leitete die örtliche Polizei ihrerseits an das **Bauordnungsamt** weiter. Nach Art. 17 Abs. 1 BayDSG wäre die Datenübermittlung an die Stadt selbst oder an das städtische Amt für öffentliche Ordnung zulässig gewesen, da sie zur rechtmäßigen Erfüllung der Aufgaben der Stadt als Sicherheitsbehörde erforderlich war. Die polizeilichen Erkenntnisse waren für die Beurteilung der Zuverlässigkeit der Betreiber im Rahmen der gaststättenrechtlichen Erlaubnis für den Diskothekenbetrieb von erheblicher Bedeutung und waren zum Zeitpunkt ihrer Übermittlung rechtmäßig gespeichert. **Unzulässig** war jedoch die Übermittlung der personenbezogenen Erkenntnisse, die für die Beurteilung im **gaststättenrechtlichen Verfahren** bestimmt waren, an das **Bauordnungsamt** der Stadt, da dieses zwar für das Baugenehmigungsverfahren, nicht aber für die Beurteilung der Zuverlässigkeit der Betroffenen und der damit zusammenhängenden Fragen der öffentlichen Sicherheit und Ordnung zuständig war. Ich habe daher die zuständige Polizeibehörde auf die fehlerhafte Zuleitung des Schreibens hingewiesen und es aufgefordert, dafür Sorge zu tragen, daß künftig Mitteilungen der Polizei an die richtigen Adressaten gerichtet werden.

Der Bericht des Polizeipräsidiums wurde vom Bauordnungsamt zum Bauakt genommen. **Die Ablage im Bauakt war in entsprechender Anwendung des Art. 16 Abs. 1 BayDSG unzulässig, da die darin enthaltenen Informationen zur rechtmäßigen Erfüllung der Aufgaben des Bauordnungsamtes offensichtlich nicht erforderlich waren.** Vielmehr hätte das Bauordnungsamt das Schreiben der Polizei im Original **ohne Einbehalten eines Abdruckes** an das Amt für öffentliche Ordnung und Straßenverkehr zur gaststättenrechtlichen Würdigung abgeben müssen. Die unzulässige Ablage im Bauakt war die entscheidende Ursache dafür, daß die Informationen aus den Kriminalakten an Unbefugte gelangen konnten.

3. **Speicherung ohne Spuren**

Ein Petent, der aufgrund eines gegen ihn geführten Ermittlungsverfahrens kurzzeitig bei der Polizei gespeichert war, begehrte Auskunft darüber, ob er wie er vermutete, in der „Terrorismusdatei" des Bundeskriminalamtes gespeichert war. Meine datenschutzrechtlichen Ermittlungen ergaben, daß das gegen den Petenten geführte Ermittlungsverfahren zu einer Speicherung seiner personenbezogenen Daten im sogenannten Kriminalaktennachweis geführt hatte. Nach der Verfahrensbeendigung durch Freispruch war die Speicherung gelöscht und die dazugehörige Kriminalakte vernichtet worden. Im Rahmen des sogenannten kriminalpolizeilichen Meldedienstes waren die personenbezogenen Daten des Petenten aber auch dem Bayerischen Landeskriminalamt gemeldet worden. Da dort zum Zeitpunkt meiner Anfrage jedoch keine Speicherungen zur Person des Petenten mehr bestanden, konnte nicht festgestellt werden, ob die Meldung zu einer **Speicherung beim Landeskriminalamt** geführt hatte. Es war auch nicht mehr feststellbar, ob die personenbezogenen Daten vom Landeskriminalamt **an das Bundeskriminalamt übermittelt** worden waren. Ich habe daher das Bundeskriminalamt gebeten, den zu APIS geführten Protokollbestand daraufhin zu überprüfen, ob eine Speicherung bzw. Löschung durch das Landeskriminalamt im Zusammenhang mit der Person des Petenten durchgeführt wurde. Zu diesem Zweck hat das Bundeskriminalamt auch seine Datensicherungsbestände ausgewertet. Trotz dieser Auswertungen konnte nicht ermittelt werden, ob der Petent jemals in APIS gespeichert war.

4. **Polizeiliche Listen mit Alkoholsündern**

Ein weiterer Petent bat mich zu überprüfen, ob es der Polizei gestattet sei, Listen derjenigen Personen und der auf diese zugelassenen Fahrzeuge zu führen, deren Führerschein sichergestellt oder eingezogen

ist, sowie Listen über Fahrer aufzustellen, die gelegentlich unter Alkoholeinfluß fahren.

Nach der Stellungnahme des Innenministeriums gibt es bei der Polizei in dem angesprochenen Bereich personenbezogene Sammlungen über die **rechtskräftige Verhängung von Fahrverboten im Zusammenhang mit Verkehrsordnungswidrigkeiten** und über **Fahrerlaubnisentziehungen.**

1. Nach dem Straßenverkehrsgesetz sind deutsche Führerscheine nach Verhängung von Fahrverboten amtlich zu **verwahren** und, falls sie nicht freiwillig herausgegeben werden, zu **beschlagnahmen.** Diese Aufgabe wurde vom Innenministerium der für den Wohnort des Betroffenen zuständigen Polizeidienststelle übertragen, soweit der Betroffene seinen Wohnsitz innerhalb Bayerns hat. Zu diesem Zweck werden die jeweiligen Polizeidienststellen von der **Zentralen Bußgeldstelle** im Bayerischen Polizeiverwaltungsamt durch einen Abdruck des Bußgeldbescheides von der Anordnung des Fahrverbotes unterrichtet. Somit verfügen die **Polizeidienststellen über Unterlagen über den im jeweiligen Dienstbereich ansässigen Personenkreis,** gegen den ein Fahrverbot ausgesprochen worden ist.

   Da Fahrverbote nicht nur wegen Alkoholdelikten, sondern häufig auch wegen Geschwindigkeitsüberschreitungen, Rotlichtverstößen oder der erheblichen Unterschreitung des erforderlichen Sicherheitsabstandes verhängt werden, stellen diese Abdrucksammlungen **keine alkoholspezifischen Unterlagen** dar. Die Vernichtung/Löschung der Daten erfolgt nach Ablauf der Fahrverbotsfrist.

   Aus datenschutzrechtlicher Sicht bestehen weder Bedenken gegen die Mitteilung der Zentralen Bußgeldstelle an die Polizei noch gegen die personenbezogene Speicherung der Fahrverbote durch die Polizei bis zum Ablauf der Fahrverbotsfrist:

   Die Datenübermittlung der Zentralen Bußgeldstelle ist rechtmäßig, da sie zur Erfüllung der oben beschriebenen Aufgabe der Polizei erforderlich ist (vgl. Art. 42 Polizeiaufgabengesetz). Die Polizei kann die personenbezogenen Daten in Akten oder Dateien speichern, da sie zur polizeilichen Aufgabenerfüllung erforderlich sind (Art. 38 Abs. 1 Polizeiaufgabengesetz).

2. Darüber hinaus werden von den Gerichten, Staatsanwaltschaften, Polizeidienststellen und Verwaltungsbehörden der für den Wohnort der betreffenden Person zuständigen Polizeidienststelle in der Regel die **Entziehung der Fahrerlaubnis** (auch die vorläufige Entziehung) mitgeteilt. Diese Datenübermittlungen sind aus datenschutzrechtlicher Sicht nicht zu beanstanden. Gleiches gilt für die Speicherung der übermittelten Daten durch die Polizei für die Dauer der Fahrerlaubnisentziehung.

   Die Datenübermittlung der Gerichte und Staatsanwaltschaften ist nach Nr. 46 der Mitteilung in Strafsachen in Verbindung mit Art. 42 Polizeiaufgabengesetz, die der Verwaltungsbehörden nach Art. 42 Polizeiaufgabengesetz zur Aufgabenerfüllung (Art. 2 Polizeiaufgabengesetz) zulässig. Die Mitteilung der Fahrerlaubnisentziehung an die für den Wohnort der betreffenden Person zuständige Polizeidienststelle ermöglicht dieser, Fahrten ohne Fahrerlaubnis zu verhindern, zu unterbinden (Gefahrenabwehr) und zu verfolgen (Strafverfolgung).

   Rechtsgrundlage für die Datenübermittlung von Polizeidienststellen an die für den Wohnort der betreffenden Personen zuständigen Polizeidienststelle ist Art. 40 Abs. 1 Polizeiaufgabengesetz. Danach kann die Polizei personenbezogene Daten an andere Polizeidienststellen übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist.

   Weitergehende Listen, Karteien oder Dateien in dem von dem Petenten angesprochenen Bereich, insbesondere mit potentiellen Alkoholsündern, werden nach Auskunft des Innenministeriums von der bayerischen Polizei nicht geführt.

5. **Datenabgleich bei Identitätsfeststellung**

   Ein Petent wurde wenige Tage vor dem Weltwirtschaftsgipfel von zwei Polizeibeamten einer Personalienfeststellung unterzogen. Nachdem er sich mittels seines Personalausweises ausgewiesen hatte, wurden seine Daten (Name, Vorname, Geburtsdatum) von den Polizeibeamten in einer Liste eingetragen und per Funk überprüft.

   Der Petent bat mich um Feststellung, ob seine Daten aufgrund der Erfassung in der Liste oder der Funküberprüfung gespeichert wurden. Des weiteren wollte er Auskunft über den Verbleib der Liste.

   Zur Sachverhaltsaufklärung war es notwendig, die beim Landeskriminalamt geführte **Protokolldatei** auswerten zu lassen. Mit Hilfe der Auswertung konnte der Polizeibeamte, der die Abfrage durchgeführt hatte, festgestellt und befragt werden. Dieser war für Einsatzkräfte der Bereitschaftspolizei tätig geworden, die eine Identitätsfeststellung nach Art. 13 Abs. 1 Nr. 3 Polizeiaufgabengesetz vorgenommen hatten. Danach kann die Polizei die Identität einer Person feststellen, wenn sie sich an einem besonders gefährdeten Objekt oder in unmittelbarer Nähe hierzu aufhält und Tatsachen die Annahme rechtfertigen, daß in oder an Objekten dieser Art Straftaten begangen werden sollen, durch die diese Objekte selbst unmittelbar gefährdet sind. Im vorliegenden Fall war der Petent in der Nähe des Kreisverwaltungsreferates, das als

besonders gefährdet eingestuft ist, angehalten worden.

Der über Funk erbetene Datenabgleich mit den polizeilichen Informationssystemen stützte sich auf Art. 43 Abs. 1 Polizeiaufgabengesetz. Er erlaubt der Polizei, die im Rahmen der Identitätsfeststellung erhobenen personenbezogenen Daten mit dem Inhalt polizeilicher Dateien abzugleichen, wenn Tatsachen die Annahme rechtfertigen, daß dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist.

Hinsichtlich des Verbleibs der „Liste" konnte der Petent beruhigt werden: Die „Liste" entpuppte sich als „Merkzettel" zur Gewährleistung einer zügigen Überprüfung und war bereits vernichtet worden. Auch in polizeilichen Dateien oder Karteien waren Daten des Petenten nicht gespeichert worden.

4.16 Gesetzentwurf zur Erprobung der Sicherheitswacht

Das Innenministerium hat einen Gesetzentwurf zur Erprobung der Sicherheitswacht vorgelegt, dem die Staatsregierung am 6. Juli 1993 zugestimmt hat. Angesichts des anhaltenden Anstiegs der Kriminalität und der wachsenden Gewaltbereitschaft in der Gesellschaft sollen die Bürger stärker in die Verantwortung für die innere Sicherheit eingebunden werden. Die Sicherheitswacht soll ein deutliches Zeichen gegen die **„Unkultur des Wegsehens"** und für die Übernahme von Mitverantwortung setzen. Die Angehörigen der Sicherheitswacht sollen die Polizei vor allem bei der Bekämpfung der **Straßenkriminalität** unterstützen. Einsatzschwerpunkte sollen öffentliche Anlagen, große und damit oft auch anonyme Wohnsiedlungen und Parkflächen sowie Haltestellen des öffentliche Personennahverkehrs sein. Die **schnelle Weitergabe gezielter Hinweise und Informationen** soll einen wirksamen Einsatz der Polizei gewährleisten. Darüber hinaus soll die Sicherheitswacht für die Bürger ein wichtiger **Ansprechpartner** in Fragen der Sicherheit sein.

Im Rahmen ihrer Aufgaben erhalten die Angehörigen der Sicherheitswacht das Recht, Zeugen zu befragen und Personalien festzustellen.

Gegenüber dem Innenministerium habe ich zu dem Gesetzentwurf aus datenschutzrechtlicher Sicht Stellung genommen. Grundsätzliche Bedenken habe ich dabei nicht erhoben, aber auf folgende Punkte hingewiesen:

- Ich habe Zweifel geäußert, ob der Landesgesetzgeber Befugnisse zur **Strafverfolgung** auf Angehörige der Sicherheitswacht übertragen kann, da die Strafprozeßordnung zumindest für die **polizeilichen** Befugnisse auf dem Gebiet der Verfolgung von Straftaten eine abschließende Regelung enthält und deshalb auch für die Ermächtigung von „Hilfspolizisten" zu strafprozessualen Maßnahmen kein Raum sein dürfte.

  Das Innenministerium hat in der Begründung des Entwurfs klargestellt, daß die Angehörigen der Sicherheitswacht von ihren durch den Gesetzentwurf eingeräumten Befugnissen nur im Rahmen der **Gefahrenabwehr** Gebrauch machen dürfen.

- Ich habe zum Vorentwurf darauf hingewiesen, daß die **Speicherung personenbezogener Daten** durch die Angehörigen der Sicherheitswacht selbst nicht geregelt ist und damit eine ausreichende Rechtsgrundlage für die nach meiner Einschätzung in der Praxis notwendigen Speicherungen fehlt. Das Innenministerium hat den Gesetzentwurf aufgrund dieses Hinweises ergänzt. Während für die **Datenübermittlung** von Angehörigen der Sicherheitswacht an **öffentliche** Stellen in Art. 7 des Entwurfs eine spezielle Regelung vorgesehen ist und für die Datenübermittlung an **nichtöffentliche** Stellen gemäß Art. 9 des Entwurfs das Polizeiaufgabengesetz Anwendung findet, richten sich die Speicherung, Veränderung, Sperrung, Löschung und Nutzung personenbezogener Daten durch Angehörige der Sicherheitswacht nach dem Bayerischen **Datenschutzgesetz.**

5. Verfassungsschutz

5.1 Vorbemerkungen

Bedrohungslage besteht fort

Seit dem letzten Berichtszeitraum (1992) hat die Bedrohung der freiheitlichen demokratischen Grundordnung durch den Linksextremismus, durch gewaltbereite rechtsextremistische Gruppierungen und Einzeltäter, durch ausländische Extremisten sowie durch Terroristen nicht nachgelassen. Nach wie vor ist mit terroristischen Aktionen einschließlich gezielter Angriffe auf Menschen zu rechnen. Die RAF hat im Berichtszeitraum zwar keine Anschläge auf Personen verübt, sich jedoch in drei Erklärungen ihrer Kommandoebene die Option auf terroristische Aktionen einschließlich gezielter Angriffe auf Menschen offengehalten. Im rechtsextremistischen Bereich war eine Welle ausländerfeindlicher Gewalt zu verzeichnen. Die neue Dimension der Bedrohung der inneren Sicherheit durch rechtsextremistische Gewalttäter bedeutet eine ernstzunehmende Gefährdung der freiheitlichen demokratischen Grundordnung. Die Urheber der dramatisch gestiegenen, bis hin zu Mord und Totschlag reichenden Gewaltakte negieren das Grundrecht ihrer Opfer auf Leben und körperliche Unversehrtheit und stellen damit die Grundlagen des demokratischen Rechtsstaates in Frage. Angesichts zunehmender rechtsextremistischer Umtriebe wäre es geradezu fatal, die Aktivitäten des Verfassungsschutzes zurückzufahren.

Ausweitung der Aufgaben

- Die öffentliche Diskussion um die Ausweitung der Aufgaben und Befugnisse der Verfassungsschutzbehörden auf die **Bekämpfung der organisierten**

Kriminalität dauert an. Im „Sicherheitspaket 94" vom 30. September 1993 schlägt der Bundesinnenminister vor, den Verfassungsschutz in die Bekämpfung der organisierten Kriminalität mit einzubeziehen:

„Unbeschadet der polizeilichen Alleinzuständigkeit für exekutive Zugriffe ist es geboten, dem Verfassungsschutz die Sammlung von Informationen über die Strukturen der organisierten Kriminalität und deren Weitergabe zu erlauben (Ergänzung der Aufgabenzuweisungsnorm § 3 Abs. 1 Bundesverfassungsschutzgesetz)."
Die Bundesregierung hat allerdings ursprüngliche Absichten, noch in dieser Wahlperiode die Kompetenzen des Verfassungsschutzes auszuweiten, wieder fallen gelassen.

- Der **Bundesrat** hat aber einen von Bayern eingebrachten Gesetzentwurf zur Stärkung des Rechtsfriedens und zur Bekämpfung des Schlepperunwesens beschlossen, der in Art. 4 eine Änderung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 Grundgesetz – G 10) vorsieht. Danach sollen **Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses** durch die Verfassungsschutzbehörden möglich sein, wenn Anhaltspunkte für den Verdacht bestehen, daß jemand Straftaten nach den §§ 129, 130 und 131 StGB (Bildung krimineller Vereinigungen, Volksverhetzung und Aufstachelung zum Rassenhaß) plant, begeht oder begangen hat.

  Die Erweiterung der Befugnisse des Verfassungsschutzes zur Brief-, Post- und Telefonüberwachung wird begründet mit der Notwendigkeit der **Vorfeldbeobachtung rechtsextremistischer Gruppierungen und Einzeltäter.** Eine wirksame Bekämpfung rechtsextremistischer, insbesondere neonazistisch motivierter sowie antisemitischer und fremdenfeindlicher Straftaten mit dem Ziel, solche zu verhüten und zu unterbinden, setze eine Beobachtung rechtsextremistischer Gruppierungen und Einzeltäter bereits weit im Vorfeld strafrechtlichen Handelns voraus, wozu der Verfassungsschutz kraft Gesetzes bestimmt sei. Die Verfassungsschutzbehörden benötigten jedoch zur Erfüllung ihrer Aufgaben der Vorfeldbeobachtung das entsprechende rechtliche Instrumentarium. Zu diesem Instrumentarium gehörten auch die im Gesetz zu Art. 10 GG vorgesehenen Befugnisse. Die Post- und Telefonkontrolle sei ein effektives Hilfsmittel zur frühzeitigen Erlangung von Informationen über bevorstehende rechtsextremistische Straftaten.

  Die **Bundesregierung** stimmt in ihrer Stellungnahme mit der Zielsetzung des Gesetzentwurfs überein. Sie unterstützt die Forderung des Bundesrates, geeignete gesetzliche Maßnahmen zu ergreifen, um extremistische und fremdenfeindliche Straftaten noch effektiver als bisher zu verhindern und zu unterbinden. Zu diesem Zweck prüfe sie, inwieweit Tatbestände der §§ 129 ff StGB in den Straftatenkatalog des G 10 einbezogen werden können.

  Die **Datenschutzkonferenz** hat sich mit dem Gesetzentwurf noch nicht befaßt. Aus meiner Sicht bestehen gegen die Verbesserung des Instrumentariums des Verfassungsschutzes gegenüber extremistischen Bestrebungen keine grundsätzlichen datenschutzrechtlichen Bedenken. Da rechtsextremistische Organisationen und Einzeltäter die freiheitliche demokratische Grundordnung gefährden, sind der **Aufgabenbereich des Verfassungsschutzes** eröffnet und die Grundvoraussetzungen für eine G-10-Maßnahmen nach Art. 1 § 1 Abs. 1 G 10 gegeben. Insbesondere sehe ich in diesem Zusammenhang **keine Abgrenzungsprobleme** zwischen Verfassungsschutz und Polizei. Während die Strafverfolgung Aufgabe der Polizei ist, dient die vorgeschlagene Gesetzesänderung **der Aufklärung im Vorfeld strafrechtlicher Relevanz** im Vollzug des Beobachtungsauftrages des Verfassungsschutzes. Ob die vom Bundesrat vorgeschlagene Erweiterung des Auftrags auf die Tatbestände der §§ 129, 130, 131 StGB erforderlich ist, bedarf – nach Vorliegen der Beurteilung der Bundesregierung – noch einer eingehenden datenschutzrechtlichen Prüfung. Zu berücksichtigen ist dabei, daß nach dem Bayer. Verfassungsschutzgesetz das Landesamt zur Beobachtung extremistischer Bestrebungen **nachrichtendienstliche Mittel** einschließlich elektronischer Aufklärungsmittel in Wohnungen einsetzen darf, so daß die Überwachung des Brief-, Post- und Fernmeldeverkehrs zur Vorfeldbeobachtung extremistischer Bestrebungen in diesen Fällen nur folgerichtig ist.

5.2 Auswirkungen des neuen Datenschutzgesetzes auf die Datenschutzkontrolle des Landesamts für Verfassungsschutz

Die Kontrollbefugnis des Landesbeauftragten für den Datenschutz wird zwar durch das neue Bayerische Datenschutzgesetz gegenüber dem derzeitigen Rechtszustand auf die Kontrolle der in Akten verarbeiteten Daten erweitert. Jedoch wird hier die Kontrolle auf eine bloße **Anlaßkontrolle** beschränkt (Art. 30 Abs. 1 Satz 2 BayDSG). Dies stellt eine **Beeinträchtigung der Datenschutzkontrolle** und damit unmittelbar des Datenschutzes der Bürger gerade in dem besonders sensiblen Bereich verdeckter Informationsgewinnung durch den Einsatz **nachrichtendienstlicher Mittel** dar. Der Einsatz solcher Mittel ist regelmäßig in besonderen Akten dokumentiert. Eine Erfassung verdeckter Datenerhebungsmaßnahmen in automatisierten Dateien erfolgt dagegen nicht.

Der Betroffene wird nur in Ausnahmefällen in der Lage sein, die für eine Anlaßkontrolle notwendigen Anhaltspunkte dafür darzulegen, daß er durch die Anwendung nachrichtendienstlicher Mittel in seinen Rechten verletzt

worden ist. Es entspricht gerade dem Sinn und Zweck verdeckter Datenerhebung, daß sie ohne Wissen des Betroffenen durchgeführt wird.

Der Landesbeauftragte selbst ist auf „Zufallsfunde" in der Akte anläßlich von Dateikontrollen, bei denen er durch Einsichtnahme in die Akten die Rechtmäßigkeit der Datenspeicherung überprüft, angewiesen. In der Regel erfährt er keine Anhaltspunkte für Datenschutzverstöße. Eine Prüfung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die aufgrund des Einsatzes nachrichtendienstlicher Mittel gewonnen wurden, ist mir daher – von der Nachprüfung im Rahmen einer Dateienkontrolle abgesehen – nicht möglich. Insbesondere kann ich nicht gezielt, nicht einmal stichprobenweise, überprüfen, ob für den Einsatz nachrichtendienstlicher Mittel die rechtlichen Voraussetzungen des Art. 6 BayVSG vorliegen.

Diese „Lücke" in der Datenschutzkontrolle wird zwar bei Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses im Rahmen des sogenannten G-10-Gesetzes und beim Einsatz von Abhörmitteln in Wohnungen durch die Zuständigkeit der **G-10-Kommission des Bayer. Landtags** (Entscheidung über die Zulässigkeit von G-10 Maßnahmen) ausgeglichen, soweit die Datenerhebung betroffen ist. Für die Anwendung anderer nachrichtendienstlicher Mittel (z.B. Observation, Einsatz geheimer Mitarbeiter) gibt es keine umfassende externe Kontrolle. Die **Parlamentarische Kontrollkommission** wird umfassend nur über die allgemeine Tätigkeit des Landesamtes für Verfassungsschutz unterrichtet. Im übrigen wird sie nur über Vorgänge von besonderer Bedeutung unterrichtet. Zeit, Ort und Umfang der Unterrichtung werden durch die politische Verantwortung der Staatsregierung bestimmt.

5.3 Erfahrungen mit dem Bayerischen Verfassungsschutzgesetz

5.3.1 Bayer. Verfassungsschutzgesetz

Die Regelungen des Bayerischen Verfassungsschutzgesetzes (BayVSG) vom 24. August 1990 zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten haben sich – wie meine Prüfungen zeigen – auch aus datenschutzrechtlicher Sicht grundsätzlich **bewährt.** Sie stellen einen angemessenen Ausgleich zwischen dem Informationsbedürfnis des Verfassungsschutzes und dem Grundrecht des Bürgers auf informationelle Selbstbestimmung dar. Das bedeutet einerseits, daß die Voraussetzungen für Eingriffe in die Rechte der Betroffenen **hinreichend klar bestimmt** sind, andererseits aber auch, daß nicht durch zu enge Tatbestände die Aufgabenerfüllung des Verfassungsschutzes unvertretbar behindert wird. Übertriebene Forderungen an die Normenklarheit durch Detailregelungen im Gesetz selbst sind nur vordergründig datenschutzfreundlich, belasten aber den Gesetzesvollzug und erschweren praktikable Lösungen unter Berücksichtigung der Besonderheiten des Einzelfalles. So halte ich es beispielsweise für ausreichend, wenn in Art. 7 und 8 BayVSG die **Speicherungsdauer** für personenbezogene Daten Erwachsener nicht durch konkrete Fristen bestimmt ist, sondern die Löschung von Daten und die Vernichtung von Unterlagen u.a. dann zu erfolgen hat, wenn ihre Kenntnis für die Erfüllung der gesetzlich festgelegten Aufgaben des Landesamtes für Verfassungsschutz (LfV) nicht mehr erforderlich ist. Die generelle Festlegung von Prüfungs- und Löschungsfristen in Richtlinien sowie die Festlegung von Fristen im einzelnen Vorgang wird von mir überwacht. Nach den Erfahrungen der jüngsten Zeit, insbesondere dem scharenweisen Auftreten jugendlicher Rechtsextremisten, ist allerdings zu überlegen, ob die in Art. 7 Abs. 2 BayVSG festgelegte Altersgrenze von 16 Jahren für die Speicherung in Dateien sachgerecht ist.

5.3.2 Auskunftserteilung durch das LfV

Die Bürger haben zwar keinen **Anspruch** auf Auskunft über die beim LfV in Dateien oder Akten gespeicherten Informationen. Hat aber eine Person **besonderes Interesse** an einer Auskunft über die zu ihrer Person gespeicherten Daten, so entscheidet das LfV nach pflichtgemäßem Ermessen über das Auskunftsbegehren. Hierauf haben die Bürger einen Rechtsanspruch. Die Voraussetzung eines „besonderen Interesses" für eine Entscheidung des LfV dient der Abwehr (systematischer) Ausforschung mit verfassungsfeindlicher Zielsetzung. In der Vergangenheit – vor Inkrafttreten des Bayerischen Verfassungsschutzgesetzes – waren zu diesem Zweck eine Vielzahl von Formblattanfragen von Mitgliedern linksextremistischer Organisationen bei Verfassungsschutzbehörden eingegangen, ohne daß ein individuelles Interesse erkennbar war.

Ein Verbot, Auskünfte auch in Fällen zu erteilen, in denen der Antragsteller ein „besonderes Interesse" an der Auskunft nicht darlegt, kann Art. 11 BayVSG zwar nicht entnommen werden. Das LfV ist in diesem Fall aber nicht verpflichtet, in der Sache selbst zu entscheiden. Für Auskünfte durch das Bundesamt für Verfassungsschutz hat der Bundestag der Bundesregierung empfohlen davon auszugehen, daß auch in Fällen, in denen die Voraussetzungen des § 15 Abs. 1 Bundesverfassungsschutzgesetz (Hinweis auf konkreten Sachverhalt, Darlegung eines „besonderen Interesses") nicht vorliegen, eine **Auskunftserteilung möglich** ist.

In der Praxis wird vom LfV die Prüfung eines Auskunftsersuchens abgelehnt, wenn ein **„besonderes Interesse"** nicht dargetan ist. Diese Verfahrensweise steht in Übereinstimmung mit der gesetzlichen Regelung, wenn an das „besondere Interesse" keine zu hohen Anforderungen gestellt werden. Es darf vom Betroffenen nicht verlangt werden, Angaben über sich zu machen, die Aktivitäten bezeichnen, die den Aufgabenbereich des LfV eröffnen (sog. Selbstbezichtigung). Ausreichend für die Entscheidung über den Auskunftsantrag ist es, wenn der Betroffene über das bei jedem Bürger gleichermaßen

vorhandene Interesse an der Speicherung seiner personenbezogenen Daten hinaus ein Interesse darlegt, das eine zusätzliche Bedeutung der Auskunft für ihn erkennen läßt. So reichen Darlegungen, wonach eine Speicherung vermutet wird, weil Bewerbungsgesuche bei Firmen abgelehnt wurden, die „Sicherheitsprüfungen" vornehmen oder entsprechende Bewerbungen beabsichtigt sind, für die Annahme eines „besonderen Interesses" aus. Gleiches gilt regelmäßig auch, wenn das Auskunftsbegehren nicht auf objektive, z.B. berufliche Nachteile, sondern auf irrationale Ängste und Befürchtungen gestützt wird.

Meine Prüfung hat ergeben, daß das LfV im Berichtszeitraum Auskunftsersuchen nur in einem Fall wegen fehlenden „besonderen Interesses" zurückgewiesen hat. Zur Begründung des „besonderen Interesses" an einer Auskunft hat das LfV vom Betroffenen „die Angabe konkreter Anhaltspunkte" zur Darlegung der angeführten „beruflichen Nachteile" verlangt. Wird vom LfV die Entscheidung über den Auskunftsantrag abgelehnt, weil ein „besonderes Interesse" nicht dargelegt ist, so hat das LfV den Betroffenen darauf hinzuweisen, daß er sich hinsichtlich der Verarbeitung personenbezogener Daten an den Landesbeauftragten für den Datenschutz wenden kann. Sollte es der Betroffene wünschen, werde ich die Rechtmäßigkeit der Verarbeitung seiner personenbezogenen Daten durch das LfV prüfen.

5.4 Generelle Prüfung 1993

Im Berichtszeitraum habe ich beim Landesamt für Verfassungsschutz wieder eine mehrtägige Prüfung verschiedener Dateien vorgenommen.

Prüfungsschwerpunkte waren insbesondere Speicherungen
- im Nachrichtendienstlichen Informationssystem NADIS der Verfassungsschutzbehörden und
- in der Vorgangsverwaltung (REGA).

Wesentliche Verstöße gegen datenschutzrechtliche Bestimmungen habe ich dabei nicht festgestellt.

1. **NADIS**

   Prüfungsansätze meiner systematischen Kontrollen von NADIS waren insbesondere Speicherungen
   - von Jugendlichen unter 16 Jahren,
   - von Jugendlichen zwischen 16 und 18 Jahren,
   - von über 70jährigen Personen,
   - bestimmter Familiennamen mit Erkenntnissen aus dem rechts- bzw. linksextremistischen Bereich
   - von Angehörigen bestimmter Berufsgruppen.

   Jugendliche unter 16 Jahren waren in NADIS nicht gespeichert. Verstöße gegen datenschutzrechtliche Bestimmungen waren nicht festzustellen. Soweit zu den Familiennamen und Angehörigen bestimmter Berufsgruppen bayerische Speicherungen überhaupt vorhanden waren, ergaben sich keine datenschutzrechtlichen Bedenken.

   Darüber hinaus habe ich mehrere Personenlisten, die ich
   - aus offen zugänglichen Quellen sowie
   - aus dem Bestand der bereits gelöschten Datei „MWG'92" des Polizeipräsidiums München (vgl. Ziff. 4.5.) zusammengestellt habe,

   auf Bestand in NADIS überprüft.

   Die Prüfung gab keinen Anlaß für eine datenschutzrechtliche Beanstandung.

2. **REGA**

   Erneut habe ich Speicherungen in der Datei REGA (EDV-unterstütztes Registratur- und Schriftgutverwaltungsverfahren) geprüft. Prüfungsgrundlage waren die bereits zur NADIS-Prüfung verwendeten Personenlisten.

   Zweck der Prüfung war
   - die Feststellung der Speicherung bestimmter Personen in Dateien oder Karteien des Landesamtes,
   - die Feststellung der Speicherung personenbezogener Daten zu bestimmten Ereignissen,
   - die Feststellung des Verbleibs der in REGA registrierten Unterlagen,
   - die Kontrolle der Rechtmäßigkeit der Speicherungen.

   Die Prüfung hat keine Anhaltspunkte für rechtswidrige Speicherungen ergeben.

   Nicht endgültig geklärt ist allerdings der Zweck, zu dem REGA verwendet wird. Davon hängen Umfang und Dauer der Speicherung ab. Hierüber bin ich mit dem Innenministerium in Verhandlungen.

5.5 Kontrolle von Einzelvorgängen

Überprüfung der Partei „Die Republikaner" mit nachrichtendienstlichen Mitteln

Presseberichte über die Überprüfung des Landesverbandes Bayern der Partei „Die Republikaner" mit nachrichtendienstlichen Mitteln durch das Bayerische Landesamt für Verfassungsschutz (LfV) sowie der Beschluß des Verwaltungsgerichts Hannover, mit welchem dem Land Niedersachsen der Einsatz nachrichtendienstlicher Mittel gegen „Die Republikaner" untersagt worden war, gaben Anlaß zu einem Informationsgespräch mit dem LfV. Ich ließ mich über die dem LfV bekannten **tatsächlichen Anhaltspunkte für Bestrebungen oder Tätigkeiten der Republikaner** unterrichten, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind. Das Vorliegen solcher Anhaltspunkte ist Voraussetzung für die Erhebung personenbezogener Daten durch **Anwendung nachrichtendienstlicher Mittel,** z.B. von V-Leuten (Art. 6 Abs. 2 Nr. 1 Bayerisches Verfassungsschutzgesetz). Die vom LfV vorgetragenen Anhaltspunkte ließen den Einsatz nachrichtendienstlicher Mittel vertretbar erscheinen. Dabei war zu berücksichtigen, daß in Bayern „Die Republikaner" nicht wie in den anderen

Ländern als Beobachtungsobjekt eingestuft sind, sondern erst als „Prüffall", einer Vorstufe vor der Qualifizierung als Beobachtungsobjekt. Auch in dieser Phase der Vorprüfung muß das LfV durch effektive Mittel in der Lage sein zu klären, ob eine Beobachtung der Partei „Die Republikaner" erforderlich ist.

Zu berücksichtigen war ferner, daß Gegenstand von nachrichtendienstlichen Maßnahmen eine durch Art. 21 Grundgesetz besonders geschützte **Partei** ist, die mit den anderen Parteien am demokratischen Wettbewerb teilnimmt. Das **Parteienprivileg** des Grundgesetzes schützt eine Partei in einer **wehrhaften Demokratie** jedoch nicht davor, daß sich die Verfassungsschutzbehörde schon in einem frühen Stadium mit ihr beschäftigt, wenn extremistische Tendenzen erkennbar werden.

Von einer datenschutzrechtlichen Detailprüfung der Rechtmäßigkeit der Anwendung nachrichtendienstlicher Mittel, insbesondere der Verhältnismäßigkeit des Einsatzes angesichts der gegebenen Verhältnisse habe ich im Hinblick auf den vom Landesverband Bayern der Partei „Die Republikaner" gegen den Freistaat Bayern angestrengten Prozeß auf Unterlassung nachrichtendienstlicher Beobachtung abgesehen. Zwar wurde dem Freistaat Bayern mit Beschluß des Verwaltungsgerichts München vom 6. Juli 1993 untersagt, bei der Erhebung von Informationen einschließlich personenbezogener Daten über den Landesverband und dessen Mitglieder nachrichtendienstliche Mittel anzuwenden. Der Bayerische Verwaltungsgerichtshof hat jedoch diesen Beschluß mittlerweile aufgehoben und die nachrichtendienstliche Beobachtung wieder zugelassen.

6. Justiz

6.1 Regelungsdefizite im Bereich der Justiz

Vor nunmehr über zehn Jahren, am 15. Dezember 1983, erging das sog. „Volkszählungsurteil" des Bundesverfassungsgerichtes. Darin stellte das Gericht fest, daß jeder Einzelne ein Grundrecht besitze, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). Zugleich legte das Gericht die Voraussetzungen für staatliche Eingriffe in dieses Grundrecht fest. Danach bedürfen Beschränkungen einer **verfassungsmäßigen gesetzlichen Grundlage,** aus der sich Voraussetzungen und Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben.

Obwohl seit diesem wegweisenden Urteil über 10 Jahre vergangen sind, werden in manchen Bereichen der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

So fehlen insbesondere ausreichende Regelungen für
- die Datenerhebung und -nutzung im **Strafvollzug,**
- die Datenübermittlung aus den bei den Amtsgerichten geführten **Schuldnerverzeichnissen,**
- die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (**Justizmitteilungen**).

Zwar wurden 1989 der Entwurf eines **Strafverfahrensänderungsgesetzes,** 1991 der Entwurf eines Gesetzes zur Änderung von Vorschriften über das **Schuldnerverzeichnis** sowie 1992 der Entwurf eines **Justizmitteilungsgesetzes** von der Bundesregierung vorgelegt. Wann und mit welchem Inhalt die Entwürfe vom Bundestag verabschiedet werden, ist derzeit nicht absehbar.

Ich weise erneut darauf hin, daß gesetzliche Regelungen in den oben genannten Bereichen überfällig sind. Statt – in Verkennung des Grundsatzes der Normenklarheit – perfektionistische, den vernünftigen Vollzug knebelnde Detailregelungen vorzusehen, die zu einer weiteren **Verkrustung der Rechtskultur** beitragen, sollte der Gesetzgeber den Mut zu **flexibleren, generalisierenden Vorschriften** fassen, welche die Justiz vor Erstarrung bewahren und ihr hinreichend Spielraum für einen am Ziel der Regelung ausgerichteten sinnvollen Vollzug und eine bedarfsgerechte Fortentwicklung des Rechts belassen.

6.2 Gesetzgebungsverfahren

6.2.1 Registerverfahrenbeschleunigungsgesetz

Die Bundesregierung hat den Entwurf eines Gesetzes zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren – Registerverfahrenbeschleunigungsgesetz (RegVBG) – vorgelegt. Durch den Entwurf soll die wirtschaftliche Entwicklung in den neuen Bundesländern gefördert werden. Er sieht zu diesem Zweck Regelungen für einen **reibungslosen Ablauf** des **Grundbuchverfahrens** sowie der Führung der übrigen für das Wirtschaftsleben wichtigen Register, namentlich des **Handelsregisters** und des **Genossenschaftsregisters,** vor.

In datenschutzrechtlicher Hinsicht sind folgende Regelungen erwähnenswert:

1. Der Entwurf enthält die Rechtsgrundlagen für die **maschinelle Führung des Grundbuches** sowie des **Handels- und des Genossenschaftsregisters.** Dabei bestimmen die Landesregierungen durch Rechtsverordnung, daß und in welchem Umfang das Grundbuch in maschineller Form als automatisierte Datei geführt wird.

   Die vorgesehenen Regelungen halte ich aus datenschutzrechtlicher Sicht für unbedenklich.

2. Der Entwurf sieht ferner die **Einrichtung eines automatisierten Verfahrens** vor, das die **Übermittlung der Daten aus dem maschinell geführten Grundbuch und aus dem Handels- und Genossen-**

schaftsregister durch Abruf (sog. Online-Anschluß) an andere Stellen ermöglicht.

Zulässigkeitsvoraussetzung für den **Online-Anschluß** an das maschinell geführte Grundbuch, der nur Gerichten, Behörden, Notaren, öffentlich bestellten Vermessungsingenieuren, an dem Grundstück dinglich Berechtigten und der Staatsbank Berlin eröffnet wird, ist u.a., daß der Abruf von Daten die in § 12 Grundbuchordnung (GBO) für das Grundbuch zulässige Einsicht (Darlegung eines „berechtigten Interesses") nicht überschreitet, und die Zulässigkeit der Abrufe auf der Grundlage einer **Protokollierung** kontrolliert werden kann.

Ich habe in meiner Stellungnahme darauf hingewiesen, daß auch die Dauer der Speicherung der protokollierten Daten geregelt werden sollte.

3. Entgegen dem ursprünglichen Diskussionsentwurf enthält der Gesetzesentwurf keine Aussagen mehr zu der von mir seit langem geforderten **Protokollierung** der **Einsichtnahme in das Grundbuch.** Diese Fragen sollen nunmehr in einem gesonderten Entwurf weiter behandelt werden. Dabei werden vom Bundesjustizministerium Überlegungen angestellt, auf das **Vorliegen eines „berechtigten Interesses" als Voraussetzung der Einsichtnahme in das Grundbuch ganz zu verzichten.** Bei jeder Eintragung müsse derjenige, der eine solche bewilligt oder begehrt, seine Zustimmung zur Veröffentlichung erteilen. Eine Dokumentation der Einsichtnahme ist nicht mehr vorgesehen.

   Ich halte einen Verzicht auf das „berechtigte Interesse" als Voraussetzung einer Grundbucheinsicht mit den grundgesetzlichen Anforderungen zur Gewährleistung des Rechtes auf informationelle Selbstbestimmung nur für schwer vereinbar und habe diese Auffassung bei einem Fachgespräch mit Vertretern der Justizverwaltungen, an dem ich in meiner Eigenschaft als Vorsitzender des Arbeitskreises Justiz teilgenommen habe, zum Ausdruck gebracht:

   Der Schutz des Persönlichkeitsrechts des Betroffenen gebietet es, daß die im Grundbuch erfaßten personenbezogenen Daten nur solchen Personen offenbart werden, die ein berechtigtes Interesse an ihrer Kenntnisnahme darlegen konnten. Eine schrankenlose Einsicht und die damit verbundene Datenübermittlung an jedermann widerspricht der Rechtsprechung des Bundesverfassungsgerichts, wonach Grundrechte insoweit beschränkt werden dürfen, als es zum Schutz des öffentlichen Interesses unerläßlich ist.

   Für die **Protokollierung** der Grundbucheinsicht habe ich folgende Verfahren vorgeschlagen, die ausreichenden Grundrechtsschutz bei **vertretbarem Arbeitsaufwand** gewährleisten:

   1. **Maschinell geführtes Grundbuch:**

      - Wird Einsicht in das maschinell geführte Grundbuch gewährt, sind Name, Vorname und Anschrift des Einsichtnehmenden sowie Datum und Grund der Einsichtnahme zu protokollieren.
      - Der Grundstückseigentümer kann **auf Antrag gebührenfrei Auskunft** darüber erhalten, wer in das Grundbuch eingesehen hat. Das Bundesministerium der Justiz regelt weiteres in einer Verwaltungsvorschrift.
      - Die Protokollbestände dürfen zum Zwecke der Datenschutzkontrolle und der Auskunftserteilung an den Grundstückseigentümer ausgewertet werden. Die Protokollierungen sind nach einem Jahr zu löschen.

      Das Justizministerium hat darauf hingewiesen, daß die Justiz mit dem vorhandenen Personal **nicht in der Lage** sei, eine gesonderte Protokollierungsdatei zu erstellen und zu führen.

   2. **Papiergrundbuch:**

      Anträge auf Grundbucheinsicht werden, nach Gemarkung und Flurstücksnummern oder alphabetisch geordnet, in **Sammelordner,** die nach Jahrgängen farblich gekennzeichnet sind, aufbewahrt. Nach Ablauf des übernächsten Kalenderjahres werden die entsprechenden Ordner ausgesondert.

      Das Justizministerium hat darauf hingewiesen, daß die Justiz mit dem vorhandenen Personal **nicht in der Lage sei,** die geforderten Anträge aufzunehmen, zu ordnen, aufzubewahren und auszusondern.

6.2.2 Jugendvollzugsgesetz

Für den Jugendstrafvollzug gibt es bisher keine bundeseinheitliche spezialgesetzliche Grundlage. Einer datenschutzrechtlichen Forderung entsprechend hat der Bundesminister der Justiz nunmehr einen Referentenentwurf für ein Jugendvollzugsgesetz vorgelegt. Die im Grundsatz begrüßenswerte Neuregelung ist in einzelnen Punkten verbesserungsbedürftig. Dabei konnte ich mich auf meine Kontrollerfahrungen im Erwachsenenstrafvollzug stützen. In meiner Stellungnahme gegenüber dem Justizministerium habe ich gefordert:

- Auf die Möglichkeit der Anbringung von **Sichtvermerken auf ausgehenden Schreiben** des Gefangenen sollte verzichtet werden. Der Auslauf eines Schreibens könnte auf einem besonderen Blatt vermerkt und dieses zu den Gefangenenakten genommen werden. Auf diese Weise könnten unnötige Bloßstellungen vermieden werden.
- **Eingehende Schreiben,** deren Weitergabe an den Gefangenen oder deren Rückgabe an den Absender nicht in Betracht kommt, sollten nicht für jeden Voll-

zugsbediensteten zugänglich aufbewahrt werden. Vorgesehen werden sollte die Verwahrung **in einem verschlossenen Begleitumschlag,** der zur Gefangenenpersonalakte genommen wird und zu dem nur besonders ermächtigte Bedienstete Zugriff haben.

- Ein **Verstoß gegen die vorgesehene Zweckbindungsregelung,** wonach die übermittelten Daten nur für die Zwecke verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt worden sind, sollte mit einer **strafrechtlichen Sanktion** belegt werden, damit die Einhaltung dieser Regelung auch tatsächlich gewährleistet ist.
- Der vorgesehene nach dem jeweiligen Aufgabenbereich der Vollzugsdienstbediensteten **differenzierte Zugriff** auf die **Gefangenenpersonalakte** erfordert einen **gegliederten Aktenaufbau,** der insbesondere Unterordner für besonders sensible Aktenteile vorsehen sollte.
- Die bisherige **Verfahrensweise** bezüglich der **Aufbewahrung von Gefangenenbüchern,** die dem urkundlichen Nachweis des Vollzuges dienen, sollte nicht beibehalten werden.
  Bisher beginnt die Aufbewahrungsfrist für das Gefangenenbuch mit dem auf das Jahr der aktenmäßigen Weglegung folgenden Kalenderjahr, was bei Gefangenenbüchern, in denen eine Vielzahl von Gefangenen verzeichnet ist, zur Folge hat, daß die Aufbewahrungsfrist erst mit dem Jahr beginnt, in dem der Vollzug **aller** darin aufgeführten Gefangenen beendet ist. Die Aufbewahrungsfrist des Gefangenenbuches ist daher von der **Dicke des Buches** abhängig und kann im Einzelfall 50 Jahre erheblich überschreiten.
- Sollte eine **bereichsspezifische Regelung polizeilicher Überprüfung von Gefangenenbesuchern,** die im Interesse der Justizvollzugsanstalt in besonderen Fällen gegenwärtig durchgeführt wird, nicht in das Gesetz aufgenommen werden, halte ich diese Maßnahme im Hinblick auf die Intensität des Eingriffs in die Rechte unbeteiligter Dritter in Zukunft für unzulässig. Es kann nicht angehen, daß eine Person, die vom Gefangenen als Besucher gewünscht wird, ohne ihr Wissen allein aufgrund der Benennung durch den Gefangenen von der Polizei, z.B. durch Befragen des sozialen Umfeldes, darauf überprüft wird, ob durch den Besuch die Sicherheit der Anstalt oder der Unterbringungszweck gefährdet wird. Derartige Überprüfungen dürfen nur nach vorheriger Einwilligung der betreffenden Person vorgenommen werden.

Auch wenn diese Verbesserungen nicht detailliert im Gesetz festgeschrieben werden müssen, so sollte der Gesetzgeber doch die Justiz in einer **generalisierenden** Vorschrift anhalten, beim Briefverkehr und der Aktenhaltung das Persönlichkeitsrecht des Gefangenen angemessen zu berücksichtigen.

6.2.3 Strafverfahrensänderungsgesetz (StVÄG)

Der von der Bundesregierung im Jahre 1989 vorgelegte Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1989 – (StVÄG 1989) sollte entsprechend der Rechtsprechung des Bundesverfassungsgerichtes zum Grundrecht auf informationelle Selbstbestimmung die gesetzlichen Grundlagen für neuartige strafprozessuale Ermittlungsmethoden schaffen. Auch sollten hergebrachte Methoden, die Verarbeitung und Nutzung polizeilicher Informationen im Strafverfahren, das Akteneinsichtsrecht sowie der Einsatz automatisierter Verfahren neu geregelt werden.

Bisher haben nur Teilbereiche, wie z.B. der Einsatz verdeckter Ermittler, verdeckter Einsatz technischer Mittel, Rasterfahndung usw., im **Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG)** Gesetzeskraft erlangt.

Nunmehr hat eine Arbeitsgruppe der Justizverwaltungen für die **polizeiliche Datenerhebung im Strafverfahren,** die Erteilung von **Auskünften,** die **Akteneinsicht,** die **Verwendung** der erhobenen Daten sowie für **Dateien** den Entwurf eines StVÄG erstellt. Ob dieser Entwurf, der in datenschutzrechtlicher Hinsicht im Vergleich zum Entwurf 1989 eine geringere Regelungsdichte aufweist, letztlich von der Bundesregierung als Gesetzentwurf vorgelegt wird, bleibt abzuwarten. Die weitere Entwicklung dieses Gesetzesvorhabens werde ich mit besonderer Aufmerksamkeit verfolgen. Die **geringere Regelungsdichte** allein ist allerdings aus der Sicht des Datenschutzes noch **kein Nachteil.** Deshalb kann ich mich der Kritik einiger Datenschutzbeauftragten, die unter Berufung auf das Gebot der Normenklarheit wieder detailliertere Regelungen gefordert haben, nicht anschließen. Schließlich dürfen die neuen Bestimmungen **nicht zu kompliziert,** sondern müssen **in der Praxis handhabbar** und **verständlich** sein und in der **Anwendung Spielraum für vernünftiges Handeln lassen.**

6.3 Kontrollen im Justizbereich nach Inkrafttreten des neuen Bayerischen Datenschutzgesetzes

Ab 1. März 1994 bestimmt sich der Umfang meiner Kontrollkompetenz bei Gerichten und Justizbehörden, z.B. Staatsanwaltschaften, Justizvollzugsanstalten, Gerichtsvollziehern, nach Art. 30 des neuen Bayerischen Datenschutzgesetzes.

6.3.1 Überblick

Nach Art. 30 Abs. 1 S. 2 unterliegt meiner Kontrollkompetenz zwar nunmehr **auch die Erhebung, Verarbeitung** und **Nutzung** von **personenbezogenen Daten,** soweit diese nur **in Akten** verarbeitet oder genutzt werden. Diese zunächst erweiterte Kontrollkompetenz wird jedoch gleichzeitig wieder stark eingeschränkt, indem die

Kontrolle des Landesbeauftragten für den Datenschutz auf eine bloße **Anlaßkontrolle** beschränkt wird, d.h. ich darf die Datenerhebung, -verarbeitung und -nutzung in/aus Akten nur kontrollieren, wenn mir ein Bürger hinreichende Anhaltspunkte dafür darlegt, daß er durch die Erhebung, Verarbeitung und Nutzung in seinen Rechten verletzt worden ist oder wenn mir selbst hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen.

Hinsichtlich personenbezogener Daten **in Dateien** ist meine **Kompetenz nicht auf eine** solche **Anlaßkontrolle beschränkt.**

Die **Erhebung** personenbezogener Daten **durch Strafverfolgungsbehörden** (Staatsanwaltschaft und Polizei) kann ich nach Art. 30 Abs. 4 BayDSG-neu jedoch **nur überprüfen,** soweit das **Strafverfahren abgeschlossen** und die Datenerhebung nicht gerichtlich überprüft wurde.

Im Hinblick auf die richterliche Unabhängigkeit umfaßt meine Kontrollbefugnis bei **Gerichten** nach Maßgabe des Art. 30 Abs. 1 S. 2 – wie bisher – lediglich deren **Tätigkeiten in Verwaltungsangelegenheiten,** nicht jedoch in Ausübung der Rechtsprechung (Art. 2 Abs. 6).

Diese gesetzliche Regelung wirkt sich auf **zukünftige Kontrollen** von Justizbehörden wie folgt aus:

6.3.2 Kontrolle von Staatsanwaltschaften

6.3.2.1 Kontrolle bei Datenverarbeitung in Dateien

Die **Zentrale Namensdatei,** die im Rahmen des DV-Verfahrens „SIJUS-STRAF-STA" geführten Verfahrensdateien (vgl. 6.4.1.3) sowie sonstige **Dateien** können nach gegenwärtiger und zukünftiger Rechtslage von mir **ohne Vorliegen eines Anlasses** überprüft werden.

Soweit ich es für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung und Nutzung personenbezogener Daten für erforderlich halte, können dabei auch die entsprechenden **Ermittlungsakten** beigezogen werden.

Der Landesbeauftragte für den Datenschutz kann die Richtigkeit der Speicherungen in der Datei überprüfen, da unrichtige Eintragungen den Betroffenen belasten können. Unrichtig sind Eintragungen in der Datei, wenn Tatsachen nicht richtig wiedergegeben sind, wenn beispielsweise die Eintragungen im maßgeblichen Akt fehlerhaft in die Datei übernommen worden sind oder wenn Namen, Anschriften etc. falsch geschrieben oder unzutreffend wiedergegeben sind. Hingegen sind die **Entscheidungen der Staatsanwaltschaft** auf Einstellung oder Anklageerhebung, **auch wenn sie fehlerhaft ergangen** sind, als **Tatsachen** zu nehmen und vom Landesbeauftragten im Rahmen einer Dateienkontrolle nicht überprüfbar, da es sich bei der Datei SIJUS-STRAF-STA ausschließlich um ein **internes Vorgangsverwaltungs- und Aktennachweissystem** handelt, in dem allein die **Tatsache** und die **Art** der Verfahrenserledigung durch die Staatsanwaltschaft dokumentiert wird. Nur soweit die Voraussetzungen einer Anlaßkontrolle nach Art. 30 Abs. 1 Satz 2 BayDSG vorliegen, kann er die im Rahmen des Strafverfahrens vorgenommenen Datenerhebungen, -speicherungen, -nutzungen und -übermittlungen überprüfen.

Bei der Prüfung der Staatsanwaltschaft bin ich in der Erfüllung meiner Aufgaben zu **unterstützen.** Mir sind alle zur Erfüllung meiner Aufgaben notwendigen Auskünfte zu geben. Auf Anforderung sind alle Unterlagen über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Einsicht vorzulegen (Art. 28 Abs. 2 BayDSG, Art. 32 Abs. 1 BayDSG-neu). Dies geht über ein bloßes Fragerecht hinaus. Wenn ich beispielsweise kontrollieren möchte, ob die Speicherung der Verfahrensbeendigung in SIJUS rechtmäßig ist und dazu eine Reihe von Speicherungen unter diesem Gesichtspunkt überprüfe, halte ich es für erforderlich, daß ich hierzu **selbst** die Vorgänge und die dazugehörenden Akten auswählen kann. Ich halte es in diesem Zusammenhang mit meiner Prüfungskompetenz als unabhängiger Landesbeauftragter für den Datenschutz **nicht für vereinbar,** wenn, wie bei der Kontrolle einer Staatsanwaltschaft geschehen, **der Generalstaatsanwalt die Vorgänge auswählt, diese im Rahmen der Dienstaufsicht selbst überprüft** und mich **am Ergebnis seiner Überprüfung teilhaben läßt.** Die externe Datenschutzkontrolle nach dem Bayerischen Datenschutzgesetz ist im Rahmen des BayDSG ihrem Wesen nach unabhängig von der Staatsanwaltschaft. Dazu gehört – wie bei der Prüfungskompetenz des Bayer. Obersten Rechnungshofes -, daß ich Einsicht in die Akten in dem Umfang nehmen kann, **den ich für erforderlich halte.** Ich hatte bisher keine Einwände, wenn bei angekündigten Kontrollen Vertreter der vorgesetzten Behörden anwesend sind. Diese Anwesenheit darf sich freilich nicht zu einer **Behinderung der unabhängigen Datenschutzkontrolle** entwickeln.

Das Bayerische Justizministerium hat darauf hingewiesen, daß die geschilderten Schwierigkeiten bei der Prüfung einer Staatsanwaltschaft auch auf damals noch nicht ausdiskutierte grundsätzliche Fragen zum Umfang der Prüfungskompetenz des Landesbeauftragten für den Datenschutz gegenüber den Staatsanwaltschaften zurückzuführen seien.

Das Justizministerium hat im übrigen zugesagt, daß die bayerischen Staatsanwaltschaften – wie allgemein schon in der Vergangenheit – den Landesbeauftragten für den Datenschutz auch künftig bei der Erfüllung seiner Aufgaben aufgeschlossen unterstützen werden. Damit stünde allerdings nicht im Einklang, wenn die Staatsanwaltschaften angeforderte Akten künftig stets über das Justizministerium vorlegen würden.

6.3.2.2 Kontrolle bei Datenverarbeitung in/aus Akten

Strafprozessuale Maßnahmen, die in das informationelle Selbstbestimmungsrecht der Betroffenen eingreifen und die **in der Verfahrensakte** – nicht aber in einer Datei – dokumentiert werden, kann ich nach dem neuen Bayer.

Datenschutzgesetz nur überprüfen, sofern mir der Betroffene **hinreichende Anhaltspunkte** für eine Verletzung in seinen Rechten darlegt oder wenn mir hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen (Art. 30 Abs. 1 Satz 2 BayDSG, sog. **Anlaßkontrolle**). Vom Vorliegen solcher Anhaltspunkte ist nach meiner Auffassung auch dann auszugehen, wenn ich z.B. aufgrund von Eingaben den Eindruck gewinne, daß die Verfahrensweise einer Staatsanwaltschaft kein Einzelfall ist und infolge dessen Rechtsverletzungen in anderen staatsanwaltschaftlichen Verfahren der gleichen oder einer anderen Behörde anzunehmen sind. In diesem Fall kann ich zur Überprüfung der mir für die Annahme von Rechtsverletzungen vorliegenden Anhaltspunkte bei der betreffenden Staatsanwaltschaft oder anderen Staatsanwaltschaften in weitere Verfahrensakten Einsicht nehmen.

Anlaßunabhängige Kontrollen von Akten ohne Dateibezug sind mir dagegen wegen der Einschränkung der Prüfkompetenz nicht möglich. Dies hat zur Folge, daß selbst **staatsanwaltschaftliche Maßnahmen, von denen der Betroffene** keine Kenntnis erhält, die aber tief in sein Persönlichkeitsrecht eingreifen, **einer stichprobenweisen Überprüfung durch den Landesbeauftragten auch dann nicht zugänglich sind, wenn keine gerichtliche Überprüfung durchgeführt wurde.** Dabei geht es einmal um verdeckte Datenerhebungsmaßnahmen der Strafverfolgungsbehörden, wie z.B. Herstellung von Lichtbildern und Bildaufzeichnungen (§ 100 c Abs. 1 Nr. 1 a StPO), sowie um den Einsatz von verdeckten Ermittlern (§ 110 a StPO). Hier findet eine externe Kontrolle durch den Landesbeauftragten praktisch nicht statt.

Gegenüber der Datenschutzkontrolle weitgehend **abgeschottet** sind auch

- **Datenübermittlungen** durch
  - **Gewährung** von **Akteneinsicht** an Dritte
  - **Mitteilungen von Verfahrensentscheidungen an die Polizei** oder **Bundeszentralregisterbehörde**, die Auswirkungen auf die Speicherung bei diesen Behörden haben können
  - **Beiziehen von nichtanonymisierten Musterentscheidungen aus anderen Verfahren** oder
  - **Unterrichtung des Anzeigeerstatters über die Gründe der Einstellung eines Verfahrens.**

  Eine fehlerhafte Praxis zu Lasten von Beschuldigten, Zeugen und Opfern wird nur per Zufall aufgedeckt.
- **Datenerhebungen** durch
  - **Beiziehen anderer Verfahrensakten oder nichtanonymisierten Musterentscheidungen aus anderen Verfahren**
  - **Einholung von Auskünften über den Betroffenen bei anderen Behörden**

Doch **selbst wenn** mir **Anhaltspunkte für** eine **Rechtsverletzung** eines Betroffenen **vorliegen** oder Prüfungsgegenstand **Dateien bzw. Karteien** sind, ist meine Kontrolle der Zulässigkeit einer **Datenerhebung** durch Polizei oder Staatsanwaltschaft bis zum Abschluß des Strafverfahrens aufgeschoben (Art. 30 Abs. 4 BayDSG). Erst wenn die Staatsanwaltschaft das Ermittlungsverfahren eingestellt hat bzw. wenn nach Anklageerhebung die Rechtskraft der gerichtlichen Entscheidung eingetreten ist, kann ich eine solche Kontrolle durchführen. Bis dahin können, gerade bei Ermittlungsverfahren, bei denen erfahrungsgemäß häufig verdeckte Ermittlungsmaßnahmen eingesetzt werden, viele Monate oder sogar Jahre verstreichen.

Auch die gerichtliche Anordnung oder nachträgliche richterliche Bestätigung einer Datenerhebung schützen nach meiner Auffassung nicht hinreichend das Persönlichkeitsrecht des Betroffenen. So überprüft der Richter z.B. bei seiner Entscheidung über die Anordnung der Telefonüberwachung nach § 100 a StPO nur, ob die gesetzlichen Voraussetzung für eine solche Maßnahme vorliegen, nicht aber die **Durchführung** der Telefonüberwachung. Eine richterliche Prüfung, ob sich die Überwachung in den gesetzlichen Grenzen hält und ob die dabei erhobenen Daten tatsächlich nach § 100 b Abs. 5 StPO vernichtet werden, erfolgt nicht.

6.3.3 Kontrolle von Justizvollzugsanstalten

Auch bei Justizvollzugsanstalten finden sich die in datenschutzrechtlicher Hinsicht besonders sensiblen personenbezogenen Speicherungen in **Akten.** So werden angehaltene Briefe, die aus der Überwachung des Schrift- und Besuchsverkehrs erlangten Erkenntnisse wie auch etwaige polizeiliche Auskünfte im Rahmen der Besucherüberprüfung in der Gefangenenpersonalakte abgelegt. Da der **Gefangene nach der geltenden gesetzlichen Regelung kein eigenes Akteneinsichtsrecht** hat, weiß er regelmäßig auch nicht, welche ggf. belastenden Informationen über ihn im einzelnen gespeichert sind. Er wird mir deshalb auch keine Anhaltspunkte für Rechtsverletzungen darlegen können. Eine datenschutzrechtliche Überprüfung der in den Akten befindlichen Daten ist folglich in den meisten Fällen nicht möglich.

6.4 Automatisierte Verfahren

6.4.1 Sijus-Strafsachen-Staatsanwaltschaft

Die datenschutzrechtliche Kontrolle einer Staatsanwaltschaft (vgl. 6.9.1.) habe ich zum Anlaß genommen, das dort verwendete EDV-Verfahren „SIJUS-STRAFSACHEN-STAATSANWALTSCHAFT" (SIJUS-STRAFSTA) einer umfassenden Überprüfung zu unterziehen.

Als Ergebnis der Prüfung konnte ich feststellen, daß das DV-Verfahren, das nur Speicherungen und Nutzungen von personenbezogenen Daten, hingegen keine Datenübermittlungen vorsieht, keinen grundsätzlichen datenschutzrechtlichen Bedenken begegnet. In den Verfahrensmasken sind allerdings einzelne Felder enthalten, deren Erforderlichkeit vom Justizministerium noch näher darzulegen ist. Die Diskussion mit dem Ministerium hierüber ist noch nicht abgeschlossen. Für das Verfahren

fehlen allerdings noch die Löschungsregelungen. Sie werden derzeit vom Justizministerium erarbeitet.

6.4.1.1 Konzeption des Verfahrens

Das automatisierte Verfahren SIJUS-STRAF-STA unterstützt den Geschäftsstellenbetrieb und die Kanzleitätigkeit der Staatsanwaltschaft und bietet zudem die Möglichkeit der Textbe- und -verarbeitung unter Verwendung von Textbausteinen; bei der Erstellung von Schriftgut kann auf die **in den Dateien gespeicherten Personen- und Verfahrensdaten** zurückgegriffen werden. Es ist nach der bundeseinheitlichen Verwaltungsvorschrift „Aktenordnung für die Geschäftsstellen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften" (AktO) konzipiert.

Gesetzliche Grundlage des Verfahrens ist §§ 160, 152 StPO i.V.m. Art. 16 Abs. 1 BayDSG.

Entsprechend der „Aktenordnung" sieht das System für die **Registrierung des Schriftgutes,** das bei der Staatsanwaltschaft anfällt oder eingeht, zwei unterschiedliche Dateien vor:

- die **Zentrale Namensdatei**
- die **Verfahrensdatei**

Da die personenbezogenen Daten der Verfahrensbeteiligten in diesen Dateien erfaßt werden, waren sie auch Schwerpunkt meiner Prüfung.

6.4.1.2 Die Zentrale Namendatei

Bei der Zentralen Namendatei handelt es sich um ein Verzeichnis, in dem **die an den Verfahren Beteiligten,** unabhängig von ihrem Status (Beschuldigter, Geschädigter, Anzeigenerstatter) **aufgenommen** werden. **Aufgabe** der **Datei** ist in erster Linie der Nachweis von anhängigen oder abgeschlossenen Verfahren und Vorgängen sowie die Unterstützung beim **Neueintrag** derselben. Sie ist Grundlage für die Erstellung von **Vorgangslisten,** die Personenstammdaten und die zu diesen Personen gehörenden Verfahrensbezüge, z.B. den jeweiligen Verfahrensstatus (Beschuldigter, Anzeigenerstatter, Geschädigter) enthalten.

Mit Hilfe des Familiennamens oder des staatsanwaltschaftlichen Aktenzeichens kann von der Geschäftsstelle festgestellt werden, ob eine Person im System als **Beteiligter** eines von der Staatsanwaltschaft betriebenen Verfahrens bereits gespeichert, und bei der Behörde eine entsprechende Verfahrensakte vorhanden ist. Dem Anwender wird – entsprechend seiner Abfrage – entweder der **Personenstammdatensatz** der betreffenden Person oder eine Aufstellung sämtlicher zu dieser Person bei der Staatsanwaltschaft erfaßten Verfahren **(Vorgangsliste), unabhängig von ihrem Verfahrensstatus** am Bildschirm gezeigt und bei Bedarf ausgedruckt.

Der Personenstammdatensatz enthält neben den Personalien wie Vor- und Familienname, Geburtsdatum, -ort, Geschlecht usw. auch das **Feld „Mutter",** in dem zur präzisen Identifizierung der Geburtsname der Mutter der Verfahrensbeteiligten gespeichert werden kann. Die **Speicherung des Geburtsnamens der Mutter** eines **Beschuldigten** begegnet keinen datenschutzrechtlichen Bedenken, da diese Angabe für die Einholung einer Auskunft über den Beschuldigten aus dem Bundeszentralregister erforderlich ist. Da der Personenstammdatensatz nicht nach der Stellung im Verfahren unterscheidet, weisen allerdings auch die für **Anzeigenerstatter und Geschädigte** vorgesehenen Datensätze dieses Feld auf, obwohl über diese Personen in der Regel keine Auskunft aus dem Bundeszentralregister eingeholt wird. Ich habe deshalb das Justizministerium um Stellungnahme zur Erforderlichkeit der Erfassung des Geburtsnamens der Mutter bei diesem Personenkreis gebeten.

Die **Vorgangsliste** dient nicht der Sachbearbeitung durch den Staatsanwalt, etwa zu einer kursorischen Beurteilung der Persönlichkeit eines Beschuldigten, sondern soll den Geschäftsstellen der Staatsanwaltschaft die **Erschließung der Verfahrensakten** ermöglichen. Datenschutzrechtliche Bedenken gegen diesen Aktennachweis bestehen nicht.

6.4.1.3 Verfahrensdateien

Eintragung der Verfahrensbeteiligten

Vor jeder Neueintragung eines Vorgangs in das System hat die Geschäftsstelle zu prüfen, **in welchem (Verfahrens-)Register** der Vorgang zu erfassen ist. Unterschieden wird nach der „Aktenordnung" zwischen

- **Js-Register** (bekannter Täter)
- **UJs-Register** (unbekannter Täter)
- **AR-Register** (Vorgänge, die nicht oder jedenfalls nicht unmittelbar auf Einleitung eines Ermittlungsverfahren gerichtet sind)
- **Hs-Register** (staatsanwaltschaftliche Zivilsachen)
- **sonstige Register**

Die in den jeweiligen Registern für die Speicherung der Verfahrensbeteiligten vorgesehenen Datenfelder habe ich überprüft. Sie sind nach meinen Feststellungen ohne Ausnahme für die staatsanwaltschaftliche Aufgabenerfüllung erforderlich.

Eintragung der Verfahrensdaten

Die Erfassung von **Verfahrensdaten** dient der **Vorgangsverwaltung** und ist Voraussetzung für die Erledigung bestimmter Aufgaben durch das System selbst, z.B. der Erstellung von **Vorgangs-** und **Ausscheidungslisten** oder des **Archivsachenverzeichnisses.**

Gespeichert werden z.B. das Registerzeichen, der Status des Verfahrens, Mittäterhinweise, der Tatvorwurf, Verfahrensstatus der beteiligten Personen sowie die gerichtliche Erledigungsart. Zusätzlich sieht das System drei **Freitextfelder für Schlagworte** vor.

Sowohl die vorgesehenen Verfahrensdaten wie auch die Freitextfelder halte ich aus datenschutzrechtlicher Sicht

grundsätzlich für unbedenklich. Ich habe jedoch gegenüber dem Justizministerium darauf hingewiesen, daß die Staatsanwaltschaften zwar grundsätzlich die Möglichkeit haben sollten, ein Verfahren anhand von **Schlagworten** zu erschließen, wenn weder Aktenzeichen noch die verfahrensbeteiligten Personen bekannt sind. In **einer Dienstanweisung** sollte aber festgelegt werden, **welche** Schlagworte in Betracht kommen, damit mißbräuchliche Schlagworte vermieden werden.

6.4.1.4 Verfahrensliste

Nach dem Neueintrag eines Verfahrens in die Zentrale Namendatei wird dem sachbearbeitenden Staatsanwalt die Akte mit der sog. **Verfahrensliste des Beschuldigten** vorgelegt. Diese enthält einen **Auszug der Verfahren aus der Zentralen Namendatei** der Behörde, bei denen der Beschuldigte in das **Js- oder in das AR-Register** eingetragen ist. Neben den Personalien werden verfahrensbezogene Daten der jeweiligen Verfahren wie z.B. Aktenzeichen, Tatvorwurf, -zeit, staatsanwaltschaftliche und gerichtliche Erledigungsart in der Liste angegeben.

Der Staatsanwalt erhält dadurch eine **Kurzinformation** über bereits früher gegen den Beschuldigten bei der Staatsanwaltschaft geführte oder noch unerledigte Verfahren und kann auf Grund dieser Information gezielt die Akten beiziehen, die er für die Sachbearbeitung des vorliegenden Verfahrens benötigt. Dies dient der Zeitersparnis und Arbeitsentlastung des Staatsanwaltes und der Geschäftsstelle. Gegen einen solchen Verfahrensausdruck bestehen keine datenschutzrechtlichen Bedenken.

6.4.2 Verfahren zur Automationsunterstützung von Schöffenangelegenheiten

Zur Unterstützung der Tätigkeiten des Richters für Schöffenangelegenheiten sowie der im Zusammenhang mit der Schöffenwahl anfallenden Verwaltungsaufgaben der Schöffengeschäftsstelle wurde ein DV-Verfahren entwickelt und nach Art. 26 BayDSG freigegeben. Das Programm bietet zu diesem Zwecke folgende Anwendungsmöglichkeiten:

- Vorbereitung und Durchführung der Schöffenwahl
- Durchführung der Schöffenauslosung
- Bearbeitung des Geschäftsanfalls der Schöffengeschäftsstelle

In meiner Stellungnahme gegenüber dem Justizministerium habe ich eine **Änderung der Löschungsregelung bezüglich der Schöffenstammdaten** gefordert. Die ursprüngliche Löschungsregelung sah vor, daß diese Daten generell nach Abschluß der vierjährigen Schöffenperiode durch den Neuaufbau der Tabelle gelöscht werden. Dies hätte aber dazu geführt, daß auch die Daten solcher Personen, die nicht in die Schöffenliste aufgenommen wurden, erst zu diesem Zeitpunkt gelöscht worden wären. Da eine so lange Speicherung nicht notwendig ist, habe ich gefordert, daß die Daten dieses Personenkreises bereits nach Abschluß der Schöffenwahl gelöscht werden sollten. Das Justizministerium hat mir dazu mitgeteilt, daß meine Forderung bei der noch zu erstellenden Dienstanweisung für das DV-Verfahren berücksichtigt wird.

6.5 Aussonderung und Vernichtung von Karteikarten der manuellen Zentralnamenkartei bei Staatsanwaltschaften

Im 13. und 14. Tätigkeitsbericht habe ich geschildert, daß ich bei Prüfungen zweier Staatsanwaltschaften festgestellt habe, daß Karteikarten weiter aufbewahrt werden, obwohl die entsprechenden Verfahrensakten bereits vernichtet wurden.

Ich habe daraufhin vom Justizministerium gefordert, Karteikarten, die als Hilfsmittel zum Auffinden von Verfahrensakten dienen, zusammen mit diesen zu vernichten, da eine weitere Aufbewahrung von Karteikarten nach Aussonderung der Akten, zu deren Auffinden sie bestimmt waren, nicht erforderlich und daher nicht zulässig ist. In diesem Zusammenhang habe ich auf die Notwendigkeit hingewiesen, die **Aufbewahrungsbestimmungen** entsprechend zu ändern, und die **Aussonderung des Karteikartenaltbestandes** in Angriff zu nehmen.

Das Justizministerium hat meinem Anliegen im Ergebnis entsprochen. Es hat nach Anhörung der staatsanwaltschaftlichen Praxis angeordnet, die Karteikarten der manuellen Zentralnamenkarteien spätestens 10 Jahre nach Einrichtung einer EDV-Anlage zur Führung der Zentralnamenkartei bei der jeweiligen Staatsanwaltschaft ohne Einzelprüfung zu vernichten, wobei die 10jährige Frist mit dem auf das Jahr der Einrichtung folgenden Jahr beginnt. Es hat darauf hingewiesen, daß in Kürze 18 von 22 Staatsanwaltschaften – einige bereits seit Jahren – die Zentralnamenkartei mittels EDV führen, so daß in absehbarer Zeit der gesamte Bestand an Karteikarten vernichtet werden wird. Eine andere Regelung zur Bereinigung des Altbestandes an Karteikarten wäre mit einem unverhältnismäßig hohen Personal- und Verwaltungsaufwand verbunden, der angesichts der angespannten Personalsituation ohne Beeinträchtigung der staatsanwaltschaftlichen Ermittlungsarbeit nicht geleistet werden könnte.

Die beabsichtigte pauschale Verfahrensweise halte ich im Hinblick auf den Verwaltungs- und Personalmehraufwand bei individueller Prüfung jeder einzelnen Karteikarte für vertretbar. Ich habe jedoch darauf hingewiesen, daß – soweit Staatsanwaltschaften noch nicht über eine EDV-Anlage verfügen – bei Neuanzeigen in Zukunft sichergestellt sein sollte, daß die **Karteikarten zusammen mit den dazugehörigen Akten** vernichtet werden.

6.6 Einsatz privater Personal Computer durch Richter und Staatsanwälte

In meinem 14. Tätigkeitsbericht habe ich gefordert, daß Staatsanwälte private Personal Computer zu dienstlichen Zwecken nur nach Anzeige an den Behördenleiter und auf der Grundlage von behördeninternen Datenschutz-

hinweisen für den konkreten Anwendungsbereich verwenden dürfen.

Das Justizministerium teilt meine Auffassung. Es hat mir mitgeteilt, daß es derzeit den Erlaß einer entsprechenden Regelung vorbereitet.

6.7 Zeugenanschriften in Bußgeldbescheiden

Im 12. Tätigkeitsbericht habe ich geschildert, daß im Zusammenhang mit einer Verbesserung des Zeugenschutzes im **Strafverfahren** in der Justiz und unter den Datenschutzbeauftragten die Frage erörtert wird, ob es nach geltendem Recht zulässig und geboten ist, in **Strafbefehlen** die vollständigen Wohn**anschriften** von Zeugen wegzulassen und nur noch deren Namen, Vornamen und evtl. den Wohnort anzugeben. Diese Frage wird nach der herrschenden Auffassung in Literatur und Rechtsprechung aus den im 12. Tätigkeitsbericht dargelegten Gründen verneint. Das Justizministerium neigt allerdings der datenschutzfreundlicheren Auffassung zu, daß die Angabe der vollständigen Wohnanschrift eines Zeugen im Strafbefehl **nicht** erforderlich sei. Dieser Auffassung schließe ich mich an.

Im Hinblick auf den gegenüber Straftaten geringeren Unrechtsgehalt von **Ordnungswidrigkeiten** ist nach meiner Auffassung ein Bedürfnis, regelmäßig die vollständige Wohnanschrift von Zeugen im **Bußgeldbescheid** aufzunehmen, um so weniger zu erkennen. Ich habe daher gegenüber dem Innenministerium angeregt, in Bußgeldbescheiden künftig lediglich den Wohn**ort** der Zeugen anzugeben.

Das **Innenministerium** hat mir mitgeteilt, daß es meine Auffassung teile, und mein Anliegen bei der nächsten Anderung der Vollzugsbekanntmachung zum Ordnungswidrigkeitengesetz berücksichtigt werde. Auch das Bayer. Polizeiverwaltungsamt werde künftig im Bußgeldbescheid regelmäßig auf die vollständige Angabe der Wohnanschrift der Zeugen verzichten.

6.8 Persönlichkeitsschutz in gerichtlichen und staatsanwaltschaftlichen Verfahren

In folgenden Bereichen des gerichtlichen und staatsanwaltschaftlichen Verfahrens sehe ich datenschutzrechtliche Defizite, die alsbald behoben werden sollten:

6.8.1 Abfassung von Einstellungsbescheiden der Staatsanwaltschaft

Stellt die Staatsanwaltschaft ein Ermittlungsverfahren ein, so hat sie nach § 171 StPO den „Anzeigenerstatter" unter Angabe der Gründe zu bescheiden. Dies gilt nach dem Wortlaut dieser Vorschrift selbst dann, wenn der Anzeigenerstatter durch die behauptete Straftat nicht in seinen Rechten verletzt ist.

Wie Bürgereingaben belegen, kann bei der Einstellung eines staatsanwaltschaftlichen Ermittlungsverfahrens das Persönlichkeitsrecht von Opfern und Zeugen durch die **Weitergabe von sensiblen Informationen** im Einstellungsbescheid an Anzeigenerstatter, z. B. über den Gesundheitszustand eines Geschädigten, infolge unzureichender Regelungen in der Strafprozeßordnung und in den Richtlinien für das Strafverfahren erheblich verletzt werden.

Deshalb habe ich in meinem 14. Tätigkeitsbericht gefordert, daß die Staatsanwaltschaft bei der Abfassung des Einstellungsbescheides das Persönlichkeitsrecht der von dem Ermittlungsverfahren Betroffenen stärker als bisher berücksichtigen sollte. Einstellungsbescheide, in denen die Staatsanwaltschaft dem Anzeigeerstatter die Gründe für die Einstellung des Ermittlungsverfahrens mitteilt, müssen so abgefaßt werden, daß sie die vorrangigen schutzwürdigen Interessen von Opfern und Zeugen einer Straftat nicht verletzen. So hat der Entscheidung, ob dem Anzeigenerstatter ein sensibles personenbezogenes Datum eines Betroffenen durch Aufnahme in den Einstellungsbescheid offenbart werden kann, eine Abwägung der widerstreitenden Interessen vorauszugehen. Ein Anzeigenerstatter hat nicht bereits aufgrund seiner formellen Beteiligung am Strafverfahren ein Recht, sensible Informationen über Zeugen und Opfer zu erhalten. Soweit es die Berücksichtigung des Persönlichkeitsrechts eines Betroffenen erfordert, ist der Einstellungsbescheid abweichend von der Begründung der Einstellungsverfügung abzufassen.

Bis zu einer entsprechenden gesetzlichen Regelung sollte daher die zu dieser Vorschrift erlassene Verwaltungsvorschrift **Nr. 89 Abs. 4 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) ergänzt** werden. Ich habe mich mit folgendem **Formulierungsvorschlag** an das Justizministerium gewandt:

> Der Staatsanwalt soll den Einstellungsbescheid so fassen, daß er auch dem rechtsunkundigen Antragsteller verständlich ist. **Bei der Entscheidung, in welchem Umfang personenbezogene Daten in den Einstellungsbescheid aufgenommen werden, sind die schutzwürdigen Interessen des Beschuldigten und anderer Personen (z. B. Opfer, Zeugen) mit denen des Anzeigenerstatters abzuwägen. Überwiegt das Interesse des Betroffenen daran, ein personenbezogenes Datum, wie etwa den Gesundheitszustand eines Opfers, dem Anzeigenerstatter nicht zu offenbaren, so ist dieses in den Bescheid nicht aufzunehmen. Bei der Gewichtung des Interesses des nichtverletzten Anzeigenerstatters ist zu beachten, daß dessen materielle Rechtsposition durch die Tat nicht betroffen ist.**
>
> **Soweit es die Berücksichtigung des Persönlichkeitsrechtes eines Betroffenen erfordert, ist der Bescheid abweichend von der Begründung der Einstellungsverfügung abzufassen.**

Das **Staatsministerium der Justiz** hat mir mitgeteilt, daß dieser Problemkreis anläßlich einer Dienstbesprechung mit den Leiterinnen und Leitern der Staatsanwaltschaften erörtert wird.

6.8.2 Akteneinsicht Dritter

Die Einsicht in Strafakten durch nichtverletzte Anzeigenerstatter und nicht am Verfahren Beteiligte ist bisher gesetzlich nicht geregelt. Sie hat ihre Grundlage derzeit noch in bundeseinheitlichen Verwaltungsvorschriften. Im Hinblick auf das durch die Einsicht berührte Grundrecht auf informationelle Selbstbestimmung der Betroffenen bedarf die Akteneinsicht Dritter in Ermittlungsverfahren dringend einer **gesetzlichen Regelung.**

Für die **Übergangszeit** kann die Gewährung der Akteneinsicht ohne ausreichende Rechtsgrundlage hingenommen werden, wenn dabei der Erforderlichkeits- und Verhältnismäßigkeitsgrundsatz strikt beachtet wird. Ich habe das Justizministerium aufgefordert dafür Sorge zu tragen, daß bei der Entscheidung über Anträge auf Akteneinsicht **folgende Grundsätze berücksichtigt** werden:

- Allein der Umstand, daß der Anzeigenerstatter Beschwerde gegen eine Einstellungsverfügung der Staatsanwaltschaft einlegen kann, rechtfertigt noch keine Akteneinsicht. Das formelle Beschwerderecht kann nicht zur Kenntnis von mehr personenbezogenen Informationen berechtigen als der Anzeigenerstatter durch den Einstellungsbescheid erhält (vgl. 6.8.1). Voraussetzung muß stets ein überwiegendes berechtigtes **materielles** Interesse sein.

  Nr. 185 Abs. 3 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) sollte daher wie folgt **ergänzt werden:**

  (Akteneinsicht kann gewährt werden) ...und wenn sonst Bedenken, **insbesondere überwiegende schutzwürdige Interessen des Beschuldigten oder anderer Personen nicht entgegenstehen.**

- Der **Antragsteller** hat sein **berechtigtes Interesse** so **darzulegen** und zu **begründen,** daß im einzelnen **erkennbar** ist, welche in der Ermittlungsakte enthaltenen Informationen von dem berechtigten Interesse **an der Übermittlung** umfaßt werden.

- Der Ermittlungsakt darf nur dann zur Akteneinsicht übersandt werden, wenn eine **Auskunft** für die Wahrnehmung der berechtigten Interessen des Antragstellers nicht genügt.

- Die **Akteneinsicht** ist grundsätzlich **auf die Aktenteile zu beschränken,** für deren Kenntnisnahme ein berechtigtes Interesse nachvollziehbar dargelegt ist.

Ich habe zudem gegenüber dem Justizministerium einen **stärkeren Schutz gegen die zweckwidrige Verwendung von Daten aus den Strafakten** gefordert. § 477 Abs. 4 StVAG-Entwurf 1989 sieht zwar vor, daß Daten, die durch Auskunft oder Akteneinsicht erlangt sind, nur zu dem Zweck verwendet werden dürfen, für den diese gewährt worden sind. Ein Verstoß gegen diesen Grundsatz bleibt jedoch nach dem vorgelegten Gesetzentwurf mangels Sanktionsnorm ohne Folgen. Ich habe daher angeregt, zum Schutze des allgemeinen Persönlichkeitsrecht § 477 Abs. 4 StVÄG mit einer **Strafbewehrung** zu versehen. Nur dann besteht die Chance, daß die Zweckbindung auch tatsächlich eingehalten wird.

Das **Staatsministerium der Justiz** teilt meine Auffassung, daß die Akteneinsicht grundsätzlich einer **gesetzlichen Regelung** bedarf. Es weist allerdings darauf hin, daß der Grundsatz der Verhältnismäßigkeit bei der Gewährung von Akteneinsicht schon von verfassungswegen zu beachten sei; die Staatsanwaltschaften seien für die Belange des Datenschutzes sensibilisiert. Bereits nach der derzeit geltenden Fassung der Nr. 185 Abs. 3 RiStBV habe eine Interessensabwägung zwischen den Interessen der Betroffenen und den Interessen dessen, der Akteneinsicht begehrt, zu erfolgen. Die Abwägung könne zu einer Beschränkung der Akteneinsicht auf bestimmte Aktenteile führen. So werde dem Interesse der Betroffenen bereits dadurch entsprochen, daß vor der Gewährung der Akteneinsicht einzelne Aktenteile, z.B. psychiatrische Gutachten, Auskünfte aus dem Bundeszentralregister, Berichte der Gerichts-, Jugendgerichts- und Bewährungshilfe, entnommen werden. In einer Besprechung der Leiterinnen und Leiter der Staatsanwaltschaft werde jedoch mein Ergänzungsvorschlag zu Nr. 185 Abs. 3 RiStBV zur Diskussion gestellt.
Keiner erhöhten Anforderungen an die **Darlegung** und **Begründung** des für die Akteneinsicht erforderlichen **„berechtigten Interesses"** bedürfe es bei den in der Praxis zahlenmäßig weit überwiegenden Akteneinsichtsgesuchen von Anwälten der Opfer und Versicherungen. Solche seien nur dann erforderlich, falls die „Opferstellung" nicht ersichtlich sei oder der Eindruck bestehe, daß die Einsicht anderen Zwecken als der Prüfung zivilrechtlicher Ansprüche diene.

Das Ministerium hält eine grundsätzliche **Ersetzung der Akteneinsicht** durch **Erteilung von Auskünften** oder Aktenauszügen nicht für durchführbar, da eine **Auskunfts- oder Aktenauszugserteilung** im Vergleich mit einer Akteneinsichtsgewährung eine höhere Arbeitsbelastung mit sich bringe und nach den Erfahrungen der Praxis der die Akteneinsicht beantragende Rechtsanwalt sich mit einer Kurzauskunft nicht zufrieden gebe.

6.8.3 Einsicht in psychiatrische Gutachten

Im 14. Tätigkeitsbericht habe ich von meinen Überlegungen zur Verbesserung des Persönlichkeitsschutzes in gerichtlichen Verfahren berichtet.

Ausgangspunkt dafür waren die von mir im 11. und 12. Tätigkeitsbericht geschilderten Fälle, in denen es in gerichtlichen Verfahren zu erheblichen Eingriffen in das Persönlichkeitsrecht der am Verfahren Beteiligten gekommen war, weil hochsensible Daten, die in psychiatrischen Gutachten enthalten waren, zur Kenntnis der anderen Verfahrensbeteiligten gelangt sind und von diesen mißbräuchlich verwendet wurden.

Zur Verbesserung des Persönlichkeitsschutzes ist es notwendig, **folgende Lücke im Gerichtsverfassungsgesetz** zu schließen:
Zwar kann das Gericht schon nach geltendem Recht den Parteien die Geheimhaltung von Tatsachen zur Pflicht machen. Ein solches **Schweigegebot,** das zusätzlich durch eine Strafandrohung abgesichert ist, kann jedoch derzeit **lediglich** bezüglich solcher Tatsachen angeordnet werden, die in einer **mündlichen Hauptverhandlung** vorgebracht wurden. Vor Durchführung einer öffentlichen Hauptverhandlung oder wenn eine solche überhaupt nicht stattfindet, ist die Anordnung nicht möglich. Dadurch sind die Betroffenen weitgehend schutzlos, da die gegnerische Partei Ergebnisse einer ärztlichen oder psychiatrischen Untersuchung ohne die Gefahr einer Bestrafung zweckwidrig verwenden kann.

Ich habe daher in meinem 14. Tätigkeitsbericht u.a. gefordert, daß **Umstände aus dem persönlichen Lebensbereich der Betroffenen, die außerhalb einer mündlichen Hauptverhandlung bekannt werden, ebenfalls der strafbewehrten Verpflichtung zur Geheimhaltung** unterliegen sollten, soweit das Gericht ein entsprechendes Schweigegebot erläßt.

Das **Justizministerium hat meine Überlegungen aufgegriffen** und gegenüber dem Bundesministerium der Justiz eine Initiative zur Ergänzung der Zivilprozeßordnung (ZPO) bzw. des Gerichtsverfassungsgesetzes (GVG) ergriffen. Einer Ergänzung des § 174 GVG als der weitergehenden, da alle Gerichtszweige umfassenden Lösung, gebe ich den Vorzug.

Ferner habe ich gegenüber dem Justizministerium darauf hingewiesen, daß nach der gegenwärtigen Rechtslage auch das **Persönlichkeitsrecht Betroffener im Rahmen einer ohnehin nichtöffentlichen Sitzung (z.B. bei Strafverhandlungen gegen Jugendliche, § 48 Jugendgerichtsgesetz) nur lückenhaft geschützt** ist. Da die Auferlegung eines Schweigegebotes nach § 174 Abs. 3 GVG den Ausschluß der Öffentlichkeit durch einen gesonderten Beschluß des Gerichtes voraussetzt, kann eine solche Anordnung bei einer ohnehin nichtöffentlichen Verhandlung vom Gericht nicht getroffen werde.

Ich habe daher angeregt, bei einer Novellierung des § 174 GVG das Schweigegebot auch auf die Fälle zu erstrecken, in denen die Hauptverhandlung ohnehin nichtöffentlich ist.

6.8.4 Überwachung des Zahlungseingangs bei Verfahrenseinstellung

Sofern den Beschuldigten bei einem Vergehen nur ein geringer Schuldvorwurf trifft, kann die Staatsanwaltschaft mit Zustimmung des Gerichts und des Beschuldigten von der Erhebung einer öffentlichen Klage absehen und das Verfahren gegen Erfüllung einer Auflage oder Weisung einstellen. Die Einstellung kann auch mit der Auflage verbunden werden, „einen Geldbetrag **zugunsten** einer gemeinnützigen Einrichtung zu zahlen" (§ 153 a Abs. 1 Nr. 2 StPO).

Dazu hat – soweit nicht entsprechende Formulare der Staatsanwaltschaft verwendet werden – der Beschuldigte, in dem **Überweisungsformular** neben seinem **Namen** und **Kontonummer** auch das **Aktenzeichen des Strafverfahrens** einzusetzen. Die Angabe des Aktenzeichens soll es der Staatsanwaltschaft ermöglichen, die Durchschrift des Überweisungsformulars, das der Beschuldigte im Regelfall als Nachweis für die Zahlung an die Staatsanwaltschaft zur endgültigen Verfahrenseinstellung zu übersenden hat, dem entsprechenden Verfahren zuzuordnen. Sofern die gemeinnützige Einrichtung im Benehmen mit der Staatsanwaltschaft die Erfüllung der Zahlungsauflage überwacht, kann sie unter Angabe des Aktenzeichens die Staatsanwaltschaft über den Zahlungseingang informieren bzw. Rückfragen der Staatsanwaltschaft beantworten. Zugleich soll die Angabe des Aktenzeichens sicherstellen, daß die gemeinnützige Einrichtung zugunsten des Beschuldigten keine Spendenbescheinigung für steuerliche Zwecke ausstellt. Bei dieser Verfahrensweise wird allerdings in Kauf genommen, daß die gemeinnützige Einrichtung von dem Strafverfahren gegen einen bestimmten Betroffenen Kenntnis erhält.

Das Justizministerium stützt diese Datenübermittlung auf § 153 a Abs. 1 Nr. 2 StPO. Sofern der Beschuldigte der Verfahrenseinstellung nach § 153 a StPO zustimme, rechne er auch mit einer Bekanntgabe seiner Personalien an den Empfänger, so daß man von einem Einverständnis des Beschuldigten zur Datenübermittlung ausgehen könne.

Demgegenüber bin ich der Auffassung, daß die gegenwärtige Praxis der Verfahrensbehandlung nach § 153 a StPO, dem gemeinnützigen Empfänger den Namen und die Anschrift des Beschuldigten sowie das Aktenzeichen des Verfahrens zu offenbaren, in § 153 a Abs. 1 StPO keine hinreichend normenklare Rechtsgrundlage findet. § 153 a Abs. 1 Nr. 2 StPO bestimmt lediglich, daß eine gemeinnützige Einrichtung Begünstigte einer Geldauflage sein kann („zugunsten"). Die Zulässigkeit einer **direkten** Leistung an die Einrichtung unter Offenbarung der personenbezogenen Daten des Beschuldigten kann der Vorschrift nicht entnommen werden, zumal es Mittel und Wege gibt, die Zahlung der Geldauflage ohne die Offenbarung des Zahlenden zu organisieren. Eine freiwillige und damit rechtswirksame Zustimmung des Beschuldigten zur Übermittlung seiner Daten an Dritte im Zusammenhang mit dem Strafverfahren sehe ich in der Zustimmung mit einer Sachbehandlung nach § 153 a StPO nicht. Dem Beschuldigten geht es vielmehr darum, eine Einstellung des gegen ihn geführten Ermittlungsverfahren zu erreichen.

Zur Vermeidung eines erheblichen Verwaltungsmehraufwandes, den eine mögliche Zahlung von Geldauflagen an die Gerichtskasse oder an die Justizzahlstelle mit sich bringen würde, habe ich vorgeschlagen, die von den Staatsanwaltschaften verwendeten **Zahl- und Überwei-**

sungsformulare so zu gestalten, daß eine Offenbarung von personenbezogenen Daten an die gemeinnützige Einrichtung unterbleiben kann. So könnten Überweisungsformulare verwendet werden, bei denen der für den Empfänger der Geldleistung bestimmte Beleg nicht im Durchschlagverfahren ausgefüllt wird. Damit bliebe dem Betroffenen überlassen, welche personenbezogene Daten er dem Empfänger der Geldauflage neben dem Aktenzeichen des Verfahrens oder einem zwischen der gemeinnützigen Einrichtung und der Staatsanwaltschaft vereinbarten Codewort offenbaren will.

Das Justizministerium teilt meine Auffassung nicht. Die Mehrheit der Landesjustizverwaltungen habe sich für die Schaffung einer gesetzlichen Grundlage für die Bekanntgabe personenbezogener Daten an gemeinnützige Einrichtungen im Zusammenhang mit der Zuweisung von Geldauflagen im Rahmen des Strafverfahrensänderungsgesetz (StVAG) ausgesprochen. Da die Offenbarung der persönlichen Daten des Beschuldigten zur Abwicklung der Verfahrenseinstellung unnötig ist, ist auch die Schaffung einer Rechtslage hierfür unnötig und daher unzulässig.

6.8.5 Eintragung der Schuldunfähigkeit in das Bundeszentralregister

Das Bundeszentralregister in Berlin enthält überwiegend Daten, die nach Abschluß eines Strafverfahrens von der Staatsanwaltschaft an die Registerbehörde übermittelt werden. Dabei betrifft die Mehrzahl der Registermeldungen Fälle, in denen es zu strafrechtlichen Verurteilungen durch Gerichte gekommen ist. In das Register werden aber auch Verfügungen der Staatsanwaltschaft eingetragen, durch die ein Strafverfahren wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit oder auf Geisteskrankheit beruhender Verhandlungsunfähigkeit ohne Verurteilung eingestellt wird. Diese Eintragungen werden nach dem Bundeszentralregistergesetz (BZRG) nur dann aus dem Register entfernt, wenn der Betroffene verstorben oder älter als 90 Jahre ist. Die Entfernung kann angeordnet werden, wenn der Betroffene ein das öffentliche Interesse an der Eintragung überwiegendes Rehabilitationsinteresse nachweist.

Nach dem Normzweck soll die Registrierung solcher Verfügungen sowohl den künftigen Entscheidungen der Gerichte, Staatsanwaltschaften und anderen Behörden als auch dem Schutze der Allgemeinheit wie dem Betroffenen selbst dienen. Diese Eintragungen erweisen sich später mitunter als unliebsame Überraschung, wenn der Betroffene bei Behörden eine Erlaubnis oder Genehmigung beantragt, bei welcher Sicherheitsbelange eine Rolle spielen.

Einen **Bescheid über die Einstellung des Ermittlungsverfahrens** und damit Kenntnis von der Annahme der Schuld- und Verhandlungsunfähigkeit durch die Staatsanwaltschaft erhält der Beschuldigte nach § 170 Abs. 2 StPO nur in den Fällen, in denen er als solcher vernommen worden ist oder Haftbefehl gegen ihn erlassen war, wenn er um einen Bescheid gebeten hat oder wenn ein **besonderes Interesse an der Bekanntgabe** ersichtlich ist. Ein solches Interesse wird bezüglich der registerrechtlichen Auswirkungen einer Einstellung des Ermittlungsverfahrens wegen Schuldunfähigkeit (Eintragung ins Bundeszentralregister) von der Justiz nicht gesehen. Da auch eine **Mitteilung der Meldung und der Eintragung** im Bundeszentralregister an den Betroffenen gesetzlich nicht vorgesehen ist, bleiben für ihn diese Auswirkungen häufig nicht überschaubar.

Dies zeigt der Fall einer Medizinstudentin, die anstatt einen Strafbefehl über 200 DM wegen eines Ladendiebstahls zu akzeptieren, Schuldunfähigkeit geltend machte und dies mit einem ärztlichen Gutachten belegte. Nach Abschluß des Studiums benötigte sie zur Approbation ein unbeschränktes Zeugnis des Bundeszentralregisters. Wegen des Eintrags der Schuldunfähigkeit hat sich die Approbationserteilung um viele Jahre verzögert.

Ich habe das Justizministerium darauf hingewiesen, daß die fehlende Unterrichtung des Betroffenen über die Eintragung der Schuldunfähigkeit in das Register **den Anforderungen des Grundrechtes auf informationelle Selbstbestimmung nicht gerecht** wird. Jeder hat ein Recht zu wissen, wer was wo über ihn weiß. Wenn jemand mit der Speicherung negativer Daten nicht rechnet, dann ist es nicht nur ein nobile officium, sondern eine Rechtspflicht der Behörde, ihn über die Speicherung zu unterrichten, falls öffentliche Belange nicht entgegenstehen. Hinsichtlich der **Speicherdauer** für den Eintrag der Schuldunfähigkeit halte ich eine **Differenzierung nach den Ursachen der Schuldunfähigkeit** für geboten. So sollte unterschieden werden, ob die Schuldunfähigkeit dauernder oder nur vorübergehender Art ist. Im Hinblick auf die weitreichenden Folgen, die ein Eintrag in das Bundeszentralregister für den Betroffenen haben kann, sollte die zuständige Staatsanwaltschaft den **Beschuldigten über die Eintragung der Einstellung des Verfahrens wegen Schuldunfähigkeit im Register belehren.**

Das Justizministerium hält mein Anliegen grundsätzlich für berechtigt. Es hat mir dazu mitgeteilt, daß das Bundesministerium der Justiz im Rahmen der Novellierung des Bundeszentralregistergesetzes auch eine umfassende Reform des § 11 BZRG plane. Dabei sei eine Lösung vorgesehen, die den Interessen der betroffenen schuldunfähigen Täter einerseits und dem Interessen der auskunftsberechtigten Stellen an einer Information über frühere Entscheidungen andererseits differenziert Rechnung tragen soll. Dem Justizministerium erscheint eine Abstufung der Speicherdauer der Eintragung nach den Ursachen der Schuldunfähigkeit erwägenswert.

Hinsichtlich meines Vorschlages, den Beschuldigten über die Eintragung im Register zu belehren, verweist das Justizministerium auf die abschließende Regelung des § 170 Abs. 2 StPO. Der Staatsanwalt habe zwar bei der Prüfung der Frage, ob ein berechtigtes Interesse des Beschuldigten an der Bekanntgabe des Verfahrensausganges ersichtlich sei, auch zu bedenken, daß in den Fäl-

len einer Einstellung, die in das Bundeszentralregister eingetragen werden, ein solches Interessen vorhanden sein könne. Eine Belehrung über die Eintragung im Bundeszentralregister sähe § 170 StPO hingegen nicht vor. Um mein Anliegen an die Praxis heranzutragen, beabsichtigt das Justizministerium diese Frage bei der nächsten Dienstbesprechung mit den Leitern der Staatsanwaltschaften zu erörtern.

6.9 Prüfungen

6.9.1 Kontrolle einer Staatsanwaltschaft

Wie im Vorjahr habe ich eine Staatsanwaltschaft geprüft, bei der das Datenverarbeitungsverfahren **„Sijus-Strafsachen"** eingesetzt wird.

Als Ergebnis der Prüfung konnte ich feststellen, daß die Staatsanwaltschaft bei der Führung der manuellen Zentralen Namenkartei sowie bei der Anwendung des DV-Verfahrens auf die Einhaltung datenschutzrechtlicher Bestimmungen achtet. Gravierende Verstöße gegen das Datenschutzrecht habe ich nicht festgestellt.

6.9.1.1 Manuelle Zentrale Namenkartei

Bis zur Einführung des DV-Verfahrens „Sijus-Strafsachen" im März 1992 wurden bei der Staatsanwaltschaft eingehende Strafverfahren in der manuellen Zentralen Namenkartei erfaßt, damit die Strafakten wieder aufgefunden werden können. Die Kartei enthält den Namen, das Geburtsdatum des Beschuldigten, den Tatvorwurf und das Aktenzeichen.

Bei datenschutzrechtlichen Kontrollen von Staatsanwaltschaften in den Berichtszeiträumen 1991 und 1992 hatte ich festgestellt, daß eine **Aussonderung und Vernichtung von Karteikarten** trotz Vernichtung der entsprechenden Verfahrensakten entweder überhaupt nicht oder nur in unzureichender Form stattgefunden hatte. Ich hatte daher gefordert, daß Karteikarten, die als Hilfsmittel zum Auffinden von Verfahrensakten dienen, zusammen mit diesen zu vernichten sind (vgl. auch 6.5).

Bei der Prüfung der Staatsanwaltschaft habe ich eine erfreuliche Aussonderungspraxis festgestellt: Seit ca. 1½ Jahren werden die Karteikarten retrograd ausgesondert, bei denen die dazugehörigen Akten bereits vernichtet wurden; in Zukunft sondert die Behörde Karteikarten zusammen mit den entsprechenden Akten aus.

6.9.1.2 Anwendung des DV-Verfahrens „Sijus-StrafStA"

Retrograde Erfassung von abgeschlossenen Verfahren in Sijus-Strafsachen

Eingehende Strafverfahren werden ab März 1992 nur noch im DV-System erfaßt und verwaltet. Eine systematische retrograde Erfassung von Verfahren, die vor diesem Zeitpunkt abgeschlossen wurden, findet nicht statt. Nur soweit beim Eingang einer Neuanzeige festgestellt wird, daß gegen den Beschuldigten bereits früher Ermittlungsverfahren durchgeführt wurden, werden die abgeschlossenen Verfahren der drei vor Einführung des DV-Systems liegenden Jahrgänge (1989–1992) retrograd erfaßt. Soweit eine retrograde Erfassung der Verfahren erfolgt, ist nach behördeninternen Anordnungen die entsprechende Karteikarte der manuellen Zentralen Namenkartei zu vernichten. Sind auf der Karteikarte mehrere Verfahren erfaßt, sind die in das DV-System übernommenen Verfahren zu schwärzen.

Bei Stichproben habe ich jedoch Verfahren festgestellt, die trotz retrograder Erfassung im DV-System noch in der manuell geführten Kartei gespeichert waren. Dies ist, so die Behörde, darauf zurückzuführen, daß die retrograde Erfassung sowohl von der Geschäftsstelle der Zentralen Namenkartei als auch von den jeweiligen Referatsgeschäftsstellen durchgeführt werden, und durch die Vielzahl der mit diesen Arbeiten befaßten Stellen die Aussonderung der Karteikarten nach Erfassung des Verfahrens im DV-System nicht immer gewährleistet ist. Ich habe daher angeregt, durch eine entsprechende Organisation der retrograden Erfassung von Altbeständen sicherzustellen, daß eine Doppelspeicherung in Zukunft vermieden wird.

Die Staatsanwaltschaft hat mittlerweile die Geschäftsstellenverwalter, die Altverfahren nur in Ausnahmefällen in das DV-System überführen, erneut dahingehend belehrt, die Übernahme von Verfahren der Zentralen Namenkartei zu melden, damit diese in die Lage versetzt sind, die entsprechenden Karteikarten zu berichtigen bzw. auszusondern.

Belegung der im System vorgesehenen Freitextfelder

Wie ich bereits oben dargelegt habe (vgl. 6.4.1.3) sehen die Verfahrensmasken des DV-Systems für die Erfassung des allgemeinen Personenstammdatensatzes der Verfahrensbeteiligten sowie für die Erfassung der Verfahrensdaten **Freitextfelder** vor. Bei Stichproben konnte ich lediglich in einem Freitextfeld eines Personenstammdatensatzes ein Datum feststellen, nämlich die Angabe der Berufsbezeichnung eines Beschuldigten.

Nach Mitteilung der Behörde dürfen in Freitextfeldern im Bedarfsfall Beiakten oder die Nummern asservierter Gegenstände, bei Verfahren gegen unbekannte Täter (UJs) das Jahr des Verfahrensbeginns und der Weglegung der Akten vermerkt werden. Die Anwender seien entsprechend belehrt worden.

Durch die Festlegung der möglichen Inhalte der Freitextfelder wird deren Verwendung datenschutzgerecht geregelt. Ich werde mich bei meinen datenschutzrechtlichen Kontrollen von der Einhaltung der Beschränkungen überzeugen.

6.9.2 Kontrolle einer Justizvollzugsanstalt

Die Vorlage eines Referentenentwurfes eines Jugendvollzugsgesetzes habe ich zum Anlaß genommen, eine Kontrolle bei einer Jugendstrafvollzugsanstalt (JVA)

durchzuführen um praktische Erfahrungen zu sammeln und etwaige Regelungsdefizite zu erkennen. Als Ergebnis konnte ich feststellen, daß die JVA dem Datenschutz einen hohen Stellenwert beimißt. Gravierende datenschutzrechtliche Mängel waren nicht festzustellen.

6.9.2.1 Gefangenenpersonalakten

Alle Informationen über einen Gefangenen sowie alle personenbezogenen Daten über Dritte (z.B Besucher, Eltern, Ehefrau), die im Strafvollzug anfallen, werden in der Gefangenenpersonalakte abgelegt. Dies gilt auch für Erkenntnisse aus der Überwachung der Gefangenenbesuche und des Schriftwechsels des Gefangenen sowie für von der JVA angehaltene Schreiben, soweit sie nicht an den Absender zurückgegeben werden. Auf die Gefangenenpersonalakte hat jeder Bedienstete der JVA jederzeit in vollem Umfang Zugriff.

Ich habe gegenüber dem Justizministerium darauf hingewiesen, daß diese Zugriffsmöglichkeit nicht den gesetzlichen Vorgaben des § 34 Abs. 2 Strafvollzugsgesetz (StVollzG) entspricht. Nach dieser Vorschrift dürfen die gewonnenen Erkenntnisse nur den **zuständigen** und nicht wahllos jedem Vollzugsbediensteten zugänglich gemacht werden. Dadurch soll die Intimsphäre des Gefangenen und betroffener Dritter bei der Informationsweitergabe innerhalb der Anstalt geschützt werden. Ich habe daher um Prüfung gebeten, auf welche Weise der gesetzlichen Regelung in der Vollzugspraxis Rechnung getragen werden kann. Bezüglich der Behandlung angehaltener Schreiben habe ich auf die Praxis in einer Erwachsenenstrafanstalt hingewiesen. Dort erfolgt die Aufbewahrung in einem verschlossenen Umschlag, auf den lediglich der Anstaltsleiter und ein von ihm Beauftragter Zugriff haben. Gründe, die gegen eine Anwendung dieses Verfahrens in einer Jugendstrafanstalt sprechen, sind nicht ersichtlich.

6.9.2.2 Gesundheitsakten

Die Gesundheitsakten der Strafgefangenen werden in einem Behandlungszimmer der Krankenabteilung in verschließbaren Aktenschränken **aufbewahrt. Zugang zu den Akten** haben der Anstaltsarzt sowie das Sanitätspersonal. Wenn sich der Arzt nicht in der Anstalt aufhält (z.B. am Wochenende), ist bei medizinischen Notfällen der Einsatz eines externen Notarztes notwendig. Da in diesen Fällen für eine optimale medizinische Versorgung des Gefangenen Informationen über seine Gesundheitsdaten aus der Gesundheitsakte erforderlich sein können, hat auch der Dienstleiter einen Schlüssel zu den Aktenschränken und damit Zugriff auf die Gesundheitsakte des Gefangenen.

Ich habe darauf hingewiesen, daß der Dienstleiter aus datenschutzrechtlichen Gründen keinen eigenen Schlüssel für die Aktenschränke, in denen die Gefangenengesundheitsakten aufbewahrt werden, besitzen sollte. Um in Notfällen den Zugriff auf die Akten auch weiterhin zu gewährleisten, habe ich vorgeschlagen, den Schlüssel in einem versiegelten Briefumschlag zu verwahren.

Die Anstalt hat meinen Vorschlag aufgegriffen und wird in Zukunft entsprechend verfahren.

6.9.2.3 Datenübermittlung an Vollstreckungsgläubiger

1. Auf schriftlichen Antrag von Gläubigern werden bei Nachweis eines **berechtigten Interesses,** das bisher durch Vorlage eines Vollstreckungstitels nachgewiesen wurde, von der JVA Auskünfte über den Gefangenen erteilt. Vor der Auskunftserteilung wird der Gefangene von der Anfrage in Kenntnis gesetzt und erhält Gelegenheit zur Äußerung. Macht er Einwände gegen die Auskunftserteilung geltend, entscheidet der Anstaltsleiter nach Abwägung der widerstreitenden Interessen. Wird Auskunft erteilt, erfolgt diese urschriftlich unter Rückgabe der Kopie des Vollstreckungstitels. Eine Dokumentation des Vorgangs findet nicht statt.

   Meine Anregung, zum Nachweis, welche Auskunft an wen erteilt und welches berechtigte Interesse vom Antragsteller dargelegt wurde, das Auskunftsersuchen sowie ein Duplikat der erteilten Auskunftsschreiben in der Akte aufzubewahren, hat die JVA aufgegriffen und wird künftig entsprechend verfahren.

2. Die JVA gibt bei der Auskunftserteilung über den Gefangenen u.a. dessen **Geburtsdatum** an.

   Die Anstalt begründet diese Verfahrensweise damit, daß die Angabe des Geburtsdatums der Identifizierung eines Gefangenen bei Namensgleichheit diene.

   Demgegenüber bin ich der Auffassung, daß es **nicht Aufgabe** der Anstalt ist, bei Gefahr einer Personenverwechslung **von sich aus zusätzliche persönliche Daten eines Gefangenen wie das Geburtsdatum zu übermitteln,** um den Gefangenen zu identifizieren. Solche Angaben können dazu führen, daß die Anstalt Daten eines Gefangenen bekannt gibt, der von der Anfrage überhaupt nicht betroffen ist.

   Ich meine daher, daß der **Auskunftsbegehrende** diejenigen Daten eines Gefangenen anzugeben hat, die es der Anstalt ermöglichen, den Gefangenen zu identifizieren. Im Zweifelsfall hat also der Auskunftsbegehrende das Geburtsdatum der Person, über die er Auskunft wünscht, zu besorgen. Soweit die Angaben nicht ausreichen, sollte die Anstalt dem Antragsteller Gelegenheit geben, diese zu ergänzen.

6.9.2.4 Besucherverkehr

Auch von der Jugendstrafvollzugsanstalt werden Personen, die von Gefangenen auf die Besucherliste gesetzt wurden polizeilich **überprüft,** sofern eine solche Maßnahme nach Auffassung der Anstalt angezeigt ist. Dies ist der Fall, wenn Verdachtsgründe vorliegen oder wenn es sich bei dem Besucher um einen ehemaligen Häftling oder einen Tatgenossen des Gefangenen handelt. Eine

Regelüberprüfung von Besuchern findet nicht statt. Im Falle einer Überprüfung holt die Anstalt fernmündlich die Auskunft der Wohnsitzpolizeiinspektion ein. Der überprüfte Besucher wird von der JVA von der Überprüfung **nicht** in Kenntnis gesetzt.

Da bisher kein Jugendvollzugsgesetz vorliegt, erfolgt die Überprüfung von Besuchern auf der Grundlage von Nr. 19 und 20 VVJug, einer (bundeseinheitlichen) Verwaltungsvorschrift zum Jugendstrafvollzug, die den Regelungen des Erwachsenenstrafvollzuges (§§ 24, 25 StVollzG) entspricht.

Ich habe bereits in meinem 14. Tätigkeitsbericht (vgl. Ziff. 6.8.6) darauf hingewiesen, daß §§ 24 und 25 StVollzG mangels Normenklarheit keine ausreichende Rechtsgrundlage für die Überprüfung darstellen und eine solche Maßnahme allenfalls auf den sog. Übergangsbonus gestützt werden kann. Eine solche Überprüfung kann zu massiven Eingriffen in das informationelle Selbstbestimmungsrecht führen, wenn etwa das soziale Umfeld des potentiellen Besuchers abgeklärt wird. Ich habe daher gefordert, bis zur Novellierung der Vorschriften über den Strafvollzug, Personen, die auf die Besucherliste gesetzt werden sollen, davon zu unterrichten, daß der Gefangene beantragt habe, sie auf die Liste zu setzen, und sie deshalb überprüft werden sollen. Erst dadurch erhält der Besucher die Möglichkeit, zu entscheiden, ob er den Gefangenen besuchen und sich deswegen überprüfen lassen will.

Demgegenüber sieht die JVA keine rechtliche oder praktische Notwendigkeit, bis zum beabsichtigten Erlaß eines Jugendvollzugsgesetzes die bisherige Praxis zu ändern.

Ich habe gegenüber dem Justizministerium zum Ausdruck gebracht, daß bis zum Erlaß eines Jugendvollzugsgesetzes die bisherige Verfahrensweise der JVA nicht uneingeschränkt weitergeführt werden kann. Denn auch auf der Grundlage des sog. Übergangsbonus sind nur solche Grundrechtseingriffe zulässig, die zur Erreichung des beabsichtigten Zweckes erforderlich sind. Eine Erforderlichkeit für die Überprüfung von Personen, bei denen noch nicht einmal feststeht, ob sie den Gefangenen besuchen wollen, kann ich aber nicht erkennen. Im übrigen habe ich darauf hingewiesen, daß der Referentenentwurf für ein Jugendvollzugsgesetz gerade keine Regelung über die polizeiliche Überprüfung von Besuchern enthält (vgl. 6.2.2).

7. Landkreise, Städte und Gemeinden

7.1 Prüfung eines Landratsamtes

1. Abrechnung privater Telefonate

Bei der Prüfung eines Landratsamtes stellte ich fest, daß die **Telefondatenerfassung** nicht den datenschutzrechtlichen Anforderungen entspricht.

Im Landratsamt waren **private** Telefongespräche über die dienstliche Telefonanlage gestattet. Zur Abrechnung dieser Telefonate wurden die Verbindungsdaten der Gespräche, die über die Vermittlung hergestellt worden waren, von der Telefonistin in eine Liste eingetragen. Sämtliche Verbindungsdaten der Gespräche, die direkt angewählt wurden, wurden maschinell ausgedruckt.

Sowohl in der Liste als auch im maschinell erstellten Ausdruck wurde die **vollständige Zielnummer** wiedergegeben. Dies ist zu Abrechnungszwecken jedoch nicht nötig. Bei der listenmäßigen Erfassung wie beim Ausdruck der Gesprächsdaten zu Abrechnungszwecken ist die Zielnummer **zu unterdrücken oder nur verkürzt auszudrucken** (z.B. ohne die letzten beiden Ziffern), damit die angerufenen Gesprächsteilnehmer unbefugten Dritten nicht bekannt werden. Zur datenschutzrechtlichen Zulässigkeit der Speicherung und Auswertung von Telefonverbindungsdaten verweise ich im übrigen auf die Veröffentlichung von Wilde/Knoblauch in der Kommunalpraxis 6/91, Seiten 210 bis 213 und auf den 14. Tätigkeitsbericht Nrn. 19.4 und 24.4.

2. Geschäftsstelle des Gutachterausschusses

Aktennotiz über mündliche Auskunft

Bei der Geschäftsstelle des Gutachterausschusses wurden die **Auskünfte an Sachverständige** aus der Kaufpreissammlung protokolliert, soweit diese Auskünfte schriftlich erteilt wurden. Sprach jedoch ein Sachverständiger persönlich vor, so wurde über die erteilte Auskunft **keine Aktennotiz** gefertigt. Zum Nachweis der Auskunftsberechtigung und zur Vermeidung mißbräuchlicher Verwendung der Auskunft sind jedoch nicht nur die schriftlichen, sondern **auch die mündlich erteilten** Auskünfte zu protokollieren.

7.2 Behandlung von Personalangelegenheiten im Gemeinderat

Im Berichtszeitraum haben mich mehrere Anfragen erreicht, die Verstöße gegen den Datenschutz bei der Behandlung von Personalangelegenheiten im Gemeinderat zum Gegenstand hatten. Im wesentlichen ging es dabei um folgende Fragen:

- **Sitzungsvorbereitung durch den ersten Bürgermeister**

  Ein Oberbürgermeister teilte mir mit, immer wieder gelangten geschützte Daten von Stellenbewerbern (Prüfungsnoten, Beurteilungen etc.), die in nichtöffentlichen Sitzungen des Stadtrats zur Sprache kämen, an die Öffentlichkeit. Die Daten seien in den den Sitzungsteilnehmern übersandten Sitzungsunterlagen enthalten gewesen. Der Oberbürgermeister wollte deshalb wissen, welche Angaben bei Einstellungen, Beförderungen u.a. den Teilnehmern nichtöffentlicher Sitzungen des Stadtrats und seiner Ausschüsse unbedingt bekannt sein müssen, ggf. in welcher Form sie ihnen mitgeteilt werden dürfen, sowie

welche Daten auf keinen Fall bekannt gegeben werden dürfen.

Bei der Behandlung von Personalangelegenheiten durch den Stadtrat und seine Ausschüsse ist das Recht auf informationelle Selbstbestimmung der Bediensteten und Stellenbewerber zu beachten. Gleichzeitig ist aber auch dem **Informationsbedürfnis des Stadtrats** Rechnung zu tragen. Denn nur ein ausreichend informierter Stadtrat kann richtige Entscheidungen treffen. Das bedeutet, daß dem Stadtrat und seinen Ausschüssen personenbezogene Daten von Bediensteten und Stellenbewerbern in dem Umfang mitgeteilt werden dürfen, als es zur Behandlung und Beschlußfassung **erforderlich** ist.

Angaben zur Person müssen in der Regel nicht über die Identifikationsdaten (Name, Alter) hinausgehen; ggf. kann der Wohnort statt genauer Adresse angegeben werden. Zurückhaltung ist geboten bei Angaben über Lebensumstände, die das soziale Umfeld beschreiben (z.B . Angaben über Ehegatten, Familienangehörige). Gesundheitsdaten im Detail dürfen, weil sie einen erheblichen Eingriff in die Intimsphäre darstellen, nicht mitgeteilt werden. Die ärztliche Feststellung, daß der Bewerber für den Dienstposten geeignet ist, reicht aus, ggf. auch die Tatsache der Behinderung.

Einzelheiten über Ausbildung und beruflichen Werdegang können je nach deren Bedeutung für die zu treffende Entscheidung angegeben werden. Dabei sollte von der Übermittlung detaillierter Daten, die der Gemeinderat nicht benötigt, abgesehen werden. Statt genauer Angaben des derzeitigen oder früheren Arbeitgebers genügt unter Umständen die Branche oder Art des Unternehmens oder Betriebs; statt einzelner Zeugnisnoten kann die Angabe einer Durchschnittsnote der relevanten Fächer genügen.

Bei einer Beförderung oder Höhergruppierung sind vorwiegend Kriterien wie Dauer der Wahrnehmung höherwertiger Aufgaben, Erfüllung der Tätigkeitsmerkmale, Dienstalter, beamtenrechtliche oder tarifvertragliche Voraussetzungen, Bewährung u. ä. für die Entscheidung notwendig.

Eine abschließende Aufzählung der zulässigen Angaben ist freilich nicht möglich, weil je nach Art der zu treffenden Entscheidung mehr oder weniger Angaben über den Betroffenen benötigt werden.

Auch bei der **Vorbereitung** und **Durchführung** der Sitzungen sind die zur Sicherung der Persönlichkeitsrechte der Bediensteten und Bewerber erforderlichen Maßnahmen zu treffen. Nach Art. 46 Abs. 2 der Gemeindeordnung bereitet der erste Bürgermeister die Beratungsgegenstände vor und beruft den Gemeinderat zu seinen Sitzungen ein. Hierbei 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. Gelangen Daten an die Öffentlichkeit, die in übersandten Sitzungsunterlagen enthalten waren, dann ist in künftigen Fällen bei der Übersendung von Sitzungsunterlagen ein strengerer Maßstab anzulegen. Der erste Bürgermeister ist regelmäßig nicht verpflichtet, in Personalangelegenheiten den Sitzungsteilnehmern vor der Beratung Sitzungsunterlagen zuzusenden. Unterlagen mit Angaben zu sensiblen, in nichtöffentlicher Sitzung zu behandelnden Gegenständen, sollten nicht versandt, sondern ggf. nummeriert als Tischvorlage für die Dauer der Sitzung zur Verfügung gestellt und anschließend wieder eingesammelt werden.

- **Bekanntgabe von Daten aus dem Personalakt eines Bediensteten im Gemeinderat**

Ein Petent bat mich, folgenden Vorgang zu überprüfen:

Seit seinem Ausscheiden aus dem Kommunaldienst hatte der Petent wiederholt geäußert, der erste Bürgermeister und die geschäftsleitende Beamtin seien nicht in der Lage, die Verwaltung ordnungsgemäß zu führen. Über diese Vorwürfe war in der örtlichen Presse berichtet worden. Die Vorwürfe des Petenten wurden auch im Gemeinderat behandelt. Da sich der Petent auf Erfahrungen aus seiner früheren Tätigkeit als Gemeindeangestellter bezog, hielt es der erste Bürgermeister zur Unterrichtung des Gemeinderats für erforderlich, in nichtöffentlicher Sitzung den Werdegang des Petenten dem der geschäftsleitenden Beamtin gegenüberzustellen. Der erste Bürgermeister ging dabei auch von der Überlegung aus, daß die Unterlagen über den Werdegang des Petenten dem Gemeinderat bei seiner Einstellung bereits vorgelegen hatten, und der Gemeinderat ein Einsichtsrecht in die Personalakten der Gemeindebediensteten hatte.

Mit dem Innenministerium bewerte ich die Angelegenheit aus datenschutzrechtlicher Sicht wie folgt: Zwar mußte sich der Gemeinderat mit den Vorwürfen des Petenten gegen den Bürgermeister und die geschäftsleitende Beamtin befassen. Aufgrund der beamtenrechtlichen Fürsorgepflicht (Art. 50 Satz 1 des Gesetzes über kommunale Wahlbeamte, Art. 86 Satz 2 des Bayerischen Beamtengesetzes) obliegt es dem Dienstherrn, Beamte gegen unberechtigte Angriffe im Zusammenhang mit ihrer dienstlichen Tätigkeit zu schützen. Der Bürgermeister durfte jedoch bei der Unterrichtung des Gemeinderats auch in nichtöffentlicher Sitzung nicht auf die Personalakten des früheren Gemeindebediensteten, des Petenten, zurückgreifen. Personalakten, die geheimhaltungsbedürftige personenbezogene Daten enthalten, genießen mit Rücksicht auf das Recht auf informatio-

nelle Selbstbestimmung der Bediensteten einen besonderen Schutz. Dieser Schutz schränkt nicht nur die Aktenübermittlung an Dritte ein, sondern erfordert auch innerhalb der Behörde Vorkehrungen, die den Kreis derer, die Kenntnis von Daten aus den Personalakten erhalten, so klein wie möglich halten. Personalakten dürfen nur im erforderlichen Umfang und entsprechend ihrer Zweckbindung als Sammlung von Vorgängen, welche die persönlichen und dienstlichen Verhältnisse der Bediensteten betreffen und in einem inneren Zusammenhang mit dem Dienstverhältnis stehen, herangezogen werden.

Im vorliegenden Fall war das Arbeitsverhältnis der Gemeinde mit dem Petenten beendet. Die Bekanntgabe von Daten aus dessen Personalakten in der Gemeinderatssitzung diente nicht einer Entscheidung im Zusammenhang mit dem Dienstverhältnis. Sie war nicht erforderlich. Auszüge aus den Personalakten des Petenten durften daher für die Beratung über die Vorwürfe gegen den Bürgermeister und die geschäftsleitende Beamtin nicht als Material herangezogen werden.

Auch die dem Gemeinderat zugewiesene Überwachungsbefugnis nach Art. 30 Abs. 3 der Gemeindeordnung erlaubt keine uneingeschränkte Einsicht in bei der Gemeinde vorhandene Unterlagen. Die Überwachungsbefugnis bezieht sich auf die Verwaltungstätigkeit der Gemeinde. Dazu hätten die Personalakten in einem Zusammenhang mit dem Kontrollrecht des Gemeinderats im Rahmen des (früheren) Arbeitsverhältnisses mit dem Petenten stehen müssen. Ein solcher Zusammenhang war jedoch nicht gegeben. Auch wenn der Petent bei seiner Kritik an der Gemeindeverwaltung auf Erkenntnisse aus seiner früheren Tätigkeit bei der Gemeinde hingewiesen hat, wurde damit seine Personalakte nicht zu einer zulässigen Informationsquelle hinsichtlich seiner Vorwürfe zur Führung der Verwaltung durch den Bürgermeister und die geschäftsleitende Beamtin.

7.3 Weitergabe von Sitzungsunterlagen

Im 14. Tätigkeitsbericht habe ich mich zur Herausgabe von Sitzungsunterlagen an die Presse und zur Mitnahme von Sitzungsunterlagen durch Gemeinderatsmitglieder geäußert (Nrn. 7.3 und 7.4). Da die Äußerungen in einem Fall zu Mißverständnissen geführt haben, möchte ich im Einvernehmen mit dem Innenministerium zur Klarstellung auf folgendes hinweisen:

- **Herausgabe von Sitzungsunterlagen an die Presse**

  Die Kommunen sind durch datenschutzrechtliche Bestimmungen nicht daran gehindert, von sich aus die Presse über Tagesordnungspunkte, die in öffentlicher Gemeinderatssitzung behandelt werden, zu unterrichten. Eine vorherige Unterrichtung der Presse kommt insbesondere in den Fällen in Betracht, in denen der Inhalt der Verwaltungsvorlage in der Gemeinderatssitzung nicht oder nur teilweise vorgetragen wird, die Angelegenheit jedoch für die Öffentlichkeit von Bedeutung ist.

  Unabhängig davon, ob sich die Presse mit einem konkreten Auskunftsersuchen an die Gemeinde gewandt hat oder diese von sich aus Auskünfte an die Presse erteilt, liegt es im **Ermessen der Gemeinde,** ob sie die Presse mündlich, fernmündlich oder durch eine vorausgehende oder nachfolgende Presseerklärung informiert. In jedem Fall hat die Gemeinde aber zu prüfen, welche Informationen zu welchen Tagesordnungspunkten sie **im Hinblick auf schutzwürdige Belange von Betroffenen** und unter Rücksichtnahme auf das Wohl der Allgemeinheit der Presse geben darf.

  Sollen personenbezogene Daten übermittelt werden, hat die Gemeinde das aus Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz abgeleitete Recht der Betroffenen auf informationelle Selbstbestimmung zu beachten. Nach den Grundsätzen des Art. 18 Abs. 1 Bayerisches Datenschutzgesetz ist eine Datenübermittlung an die Presse ohne Einwilligung der Betroffenen nur zulässig, wenn die Presse ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht, und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Will die Gemeinde die Presse durch Übermittlung von Sitzungsvorlagen über Tagesordnungspunkte unterrichten, die in öffentlicher Gemeinderatssitzung behandelt werden, dann muß sie diese Sitzungsvorlagen unter Beachtung der o.g. Grundsätze des Art. 18 Abs. 1 Bayerisches Datenschutzgesetz durch Kürzen, Schwärzen etc. so abändern, daß sie nur noch Informationen enthalten, die ohne Bedenken der Öffentlichkeit zugänglich gemacht werden dürfen.

- **Unterrichtung der Gemeinderatsmitglieder und Mitnahme von Sitzungsunterlagen**

  In Nr. 7.4 des 14. Tätigkeitsberichts unterstütze ich die Empfehlung des Innenministeriums, daß Unterlagen, die Angaben über besonders sensible, in nichtöffentlicher Sitzung zu behandelnde Beratungsgegenstände enthalten, lediglich als Tischvorlagen für die Dauer der Sitzung zur Verfügung gestellt werden sollten. Weiter vertrete ich die Auffassung, daß die Anlegung „privater" Akten und Dateien durch Mandatsträger nicht erforderlich und im übrigen sogar in höchstem Maße bedenklich ist.

  Mit diesen Äußerungen sollte keineswegs den Gemeinden bzw. dem die Sitzung vorbereitenden ersten Bürgermeister die Möglichkeit eines flexiblen Vorgehens genommen werden. Es wurden lediglich **Empfehlungen** gegeben, wie von vornherein durch praktische Maßnahmen ein Bruch der Verschwiegenheitspflicht möglichst vermieden werden kann. Daß derartige Empfehlungen notwendig sind, zeigen wiederholte Anfragen von Bürgermeistern, die um Rat-

schläge gebeten haben, weil bei ihnen trotz Hinweises auf die Geheimhaltungspflicht nach Art. 20 Abs. 2 GO immer wieder vertrauliche Informationen von einzelnen Gemeinderatsmitgliedern an unbefugte Dritte weitergegeben worden sind. Je sensibler und damit häufig je interessanter die geheimhaltungsbedürftigen Daten sind, desto größer sind die Gefahr und die Versuchung für einzelne Gemeinderatsmitglieder, sie unter Verstoß gegen ihre Pflichten weiterzugeben. Deshalb war vorgeschlagen worden, für „besonders sensible" Daten besondere Vorkehrungen zu treffen. Es sollte damit aber keine neue Kategorie geheimhaltungspflichtiger Daten eingeführt werden. Die Empfehlungen des Staatsministeriums des Innern und des Landesbeauftragten für den Datenschutz sind Ausprägungen des allgemeinen Grundsatzes, daß um so vorsichtiger vorgegangen werden sollte, je größer die Gefahr der Verschwiegenheitspflichtverletzung ist.

Mit den Empfehlungen im 14. Tätigkeitsbericht, die das geschärfte Datenschutzbewußtsein der Bürger berücksichtigen, wird deshalb auch nicht die kommunale Selbstverwaltung eingeschränkt. Sie sollen vielmehr dazu beitragen, erhebliche rechtliche Risiken, Ärger und Unannehmlichkeiten zu vermeiden.

7.4 Bekanntgabe von Einwendungsführern in öffentlicher Sitzung

Ein Bürger beschwerte sich darüber, daß durch eine Äußerung des Bürgermeisters bei der Behandlung von Einwendungen gegen die Errichtung eines Kinderspielplatzes in öffentlicher Sitzung des Gemeinderats für die örtliche Bevölkerung erkennbar geworden sei, daß der Petent die Einwendungen erhoben hatte. Ich habe ihm folgende datenschutzrechtliche Bewertung der Angelegenheit mitgeteilt:

Nach Art. 40 Abs. 1 des Gesetzes über kommunale Wahlbeamte hat der Bürgermeister über Angelegenheiten, die ihm bei seiner amtlichen Tätigkeit bekannt geworden sind, Verschwiegenheit zu bewahren, es sei denn, es handelt sich um Mitteilungen im amtlichen/dienstlichen Verkehr oder um Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Bei der Frage, ob eine Tatsache geheimhaltungsbedürftig ist oder aufgrund besonderer Rechtsvorschriften nicht der Amtsverschwiegenheit unterliegt, sind regelmäßig die Vorschriften der Bayerischen Gemeindeordnung und des Bayerischen Datenschutzgesetzes heranzuziehen.

Die Behandlung der Einwendungen des Petenten gegen den Kinderspielplatz in öffentlicher Sitzung des Gemeinderats war nach der Gemeindeordnung zu beurteilen, die nach Art. 2 Abs. 2 des Bayerischen Datenschutzgesetzes dem allgemeinen Datenschutzgesetz vorgeht.

Nach Art. 55 Abs. 2 i.V.m. Art. 52 Abs. 2 der Gemeindeordnung sind die Sitzungen öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche einzelner entgegenstehen. Bauangelegenheiten und Nachbareinwendungen gegen Bauvorhaben sind grundsätzlich in öffentlicher Gemeinderatssitzung zu behandeln. Ein generelles Geheimhaltungsinteresse der Nachbarn hinsichtlich ihrer Einwendungen zu Bauvorhaben besteht im allgemeinen nicht. Lediglich wenn ausnahmsweise Rücksichten auf das Wohl der Allgemeinheit oder berechtigte Interessen einzelner einer öffentlichen Behandlung entgegenstehen, wird in nichtöffentlicher Sitzung beraten und entschieden. Im Einzelfall kann aufgrund besonderer Umstände ein solches berechtigtes Interesse der Nachbarn an einer nichtöffentlichen Behandlung bestehen.

Im vorgetragenen Fall konnte ich ein derartiges Interesse nicht erkennen. Zur Beurteilung der Genehmigungsfähigkeit des Kinderspielplatzes mußten die Mitglieder des Gemeinderats über die Einwendungen des Petenten unterrichtet werden. Dabei wäre es auch zulässig gewesen, wenn der Bürgermeister in der Sitzung den Namen und die Adresse des Petenten genannt hätte, denn die volle Adresse ist in der Regel erforderlich, um beurteilen zu können, ob nachbarliche Belange berührt bzw. verletzt sein können. Es war deshalb aus datenschutzrechtlicher Sicht nicht zu beanstanden, daß durch die Äußerung des Bürgermeisters in der Sitzung erkennbar war, daß der Petent Einwendungen gegen den Kinderspielplatz erhoben hatte. Wer bei der Gemeinde Einwendungen gegen ein Vorhaben erhebt, muß grundsätzlich damit rechnen, daß er zur sachgerechten Erörterung seiner Einwendungen im Gemeinderat namentlich genannt wird; er kann sich nicht hinter dem Datenschutz verstecken.

7.5 Weitergabe von Daten aus dem Bautenbuch und dem Hauseigentümerverzeichnis zur Ermittlung von Vergleichsmieten

Eine Gemeindeverwaltung bat mich um Auskunft, ob sie berechtigt ist, einem Vermieter zur Ermittlung von Vergleichsmieten drei oder vier Grundstückseigentümer mitzuteilen, die ein Wohngebäude in einem bestimmten Jahr gebaut oder vermietet haben. Die Gemeinde könne diese Angaben aus dem Bautenbuch und dem Hauseigentümerverzeichnis ermitteln.

Eine Auskunft aus dem Bautenbuch und dem Hauseigentümerverzeichnis ohne die Einwilligung des Betroffenen halte ich für unzulässig. Als Rechtsgrundlage für die Datenübermittlung an den anfragenden Vermieter ist Art. 18 Abs. 1 BayDSG heranzuziehen. Die Voraussetzungen des Art. 18 Abs. 1 Alternative 1 liegen nicht vor, da die Gemeinde nicht durch Rechtsnorm verpflichtet ist, Auskünfte über Vergleichsmieten zu erteilen. Die allgemeine Verpflichtung der Gemeinden zur Erstellung eines Mietspiegels nach § 2 Abs. 5 des Gesetzes zur Regelung der Miethöhe bleibt hiervon unberührt. Auch die Voraussetzungen des Art. 18 Abs. 2 Alternative 2 sind nicht gegeben. Von seiten des Vermieters kann zwar ein berechtigtes Interesse an der Kenntnis der Informationen aus dem Bautenbuch und dem Hauseigentümerverzeichnis glaubhaft gemacht

werden. Der Auskunftserteilung stehen jedoch schutzwürdige Belange der Hauseigentümer an der Nichtpreisgabe von persönlichen Verhältnissen, z.B. die Vermieter- oder Hausbesitzereigenschaft, entgegen.

Unbedenklich wäre es hingegen, die in Frage kommenden Grundstückseigentümer anzuschreiben und um Einwilligung zur Datenübermittlung zu bitten.

7.6 Angabe von personenbezogenen Daten in der Tagesordnung zu nichtöffentlichen Sitzungen

Ein Bürger fragte bei mir an, ob in der Tagesordnung zu einer nichtöffentlichen Sitzung eines Gemeinderats der Name eines Antragstellers auf Stundung einer Gewerbesteuernachzahlung genannt werden darf.

Das halte ich für zulässig. Nach Art. 46 Abs. 2 GO beruft der erste Bürgermeister den Gemeinderat unter Angabe der Tagesordnung ein. Die Tagesordnung soll es den einzelnen Gemeinderatsmitgliedern ermöglichen, sich auf die Sitzung vorzubereiten. Die Beratungsgegenstände sind daher einzeln und konkret zu benennen. Pauschale Bezeichnungen genügen hierzu nicht. Bei der Entscheidung über den Antrag eines Bürgers ist deshalb in der Regel auch dessen Name in der Tagesordnung anzugeben.

Die Tatsache, daß Anträge auf Steuerstundungen wegen ihrer Geheimhaltungsbedürftigkeit in nichtöffentlichen Sitzungen zu behandeln sind, steht der Angabe des Namens der Betroffenen nicht entgegen, da die **Tagesordnung zu nichtöffentlichen Sitzungen nicht veröffentlicht wird,** und im übrigen die Gemeinderatsmitglieder gemäß Art. 20 GO zur Verschwiegenheit verpflichtet sind. Im Rahmen dieser Verschwiegenheitspflicht hat das einzelne Gemeinderatsmitglied dafür Sorge zu tragen, daß die Ladung zu einer nichtöffentlichen Sitzung nicht von unbefugten Dritten eingesehen werden kann.

7.7 Gewinnspiel zur Ermittlung des „freundlichsten" oder „unfreundlichsten" Gemeindebürgers

Ein bekannter Urlaubsort wollte ein Gewinnspiel für seine Kurgäste durchführen, bei dem die Gäste selbständige Unternehmer, Angestellte von Dienstleistungsunternehmen und Bedienstete öffentlicher Stellen, die ihnen als besonders freundlich oder besonders unfreundlich auffallen, benennen sollten. Hierzu sollten die Gäste den Namen des Freundlichsten bzw. Unfreundlichsten in einen Coupon eintragen, der mit dem Gästepaß an die Kurgäste verteilt wurde, und diesen bei der Kurverwaltung abgeben. Gleichzeitig war beabsichtigt, die Angaben der Gästen zu ihrem Aufenthalt (Dauer, Unterkunft usw.) mit den Gästemeldescheinen zu vergleichen und so die ordnungsgemäße Abführung der Kurabgabe zu überprüfen.

- **Ermittlung der „freundlichsten" bzw. „unfreundlichsten" Person**

  Ich habe der Gemeinde mitgeteilt, daß es für eine Erhebung und Speicherung der Namen der „freundlichsten" oder „unfreundlichsten" Bürger durch die Gemeinde keine Rechtsgrundlage gibt. Eine derartige Erhebung wird nicht mehr von der Aufgabenzuweisung der Art. 7, 57 Abs. 1 GO gedeckt, wonach die Gemeinde alle Angelegenheiten der örtlichen Gemeinschaft regeln kann und u.a. Einrichtungen nach den örtlichen Verhältnissen schaffen soll, die für das wirtschaftliche Wohl der Einwohner erforderlich sind. Bei Gemeinden, bei denen der Fremdenverkehr ein bedeutender Wirtschaftsfaktor ist, zählt hierzu zwar auch die Förderung des Fremdenverkehrs. Jedoch gibt diese Aufgabe keine Befugnis für eine allgemeine Erhebung von Daten über die Freundlichkeit bzw. Unfreundlichkeit der Gemeindebürger.

  Eine solche Erhebung **ohne Einwilligung** verletzt das allgemeine Persönlichkeitsrecht des Betroffenen. Daran ändert auch die Tatsache nichts, daß vom jeweils betroffenen Bürger vor einer Veröffentlichung der Gewinnspielauswertung dessen Zustimmung eingeholt werden sollte, da es bereits für die Datenerhebung und -speicherung an einer Rechtsgrundlage fehlt.

  Für zulässig halte ich, wenn der betroffene Bürger entweder auf dem Coupon seine Einwilligung erteilt oder diesen selbst bei der Kurverwaltung abgibt. Die beiden Möglichkeiten kommen naturgemäß nur für die Nennung einer "freundlichen Person" in Betracht. Die Gewinnspielcoupons müßten also entsprechend gestaltet werden; dabei müßte auch ein Hinweis auf die Freiwilligkeit der Teilnahme an der Aktion aufgenommen werden.

- **Vergleich der Angaben des Gastes auf dem Coupon mit den Meldedaten**

  Mit dem beabsichtigten Vergleich der Daten der Teilnehmer am Gewinnspiel mit denen der Gästeanmeldungen verfolgte die Gemeinde letztlich das Ziel, Verstöße gegen die Kurbeitragspflicht festzustellen. Im Coupon wollte sie nur auf den Abgleich der Daten des Gewinnspiels mit den Gästeanmeldungen hinweisen. Aus einem solchen Hinweis wird aber für den Teilnehmer am Gewinnspiel der Zweck dieses Vergleichs, Verstöße gegen die Kurbeitragspflicht festzustellen, nicht hinreichend klar ersichtlich, so daß es an der erforderlichen Einwilligung der Kurgäste in die Verwendung ihrer Angaben zur Überprüfung der Kurbeitragspflicht fehlt. Der Hinweis muß so gefaßt werden, daß für die Mitspieler erkennbar ist, daß der Vergleich der Feststellung dient, ob die Kurbeitragspflicht ordnungsgemäß erfüllt wird.

7.8 Bekanntgabe von Anzeigeerstattern

Von Bürgern und Gemeinden wurde ich um Auskunft gebeten, ob die Gemeinden berechtigt sind, dem Angezeigten die Auskunft über den Anzeigeerstatter zu verweigern.

1. In Betracht kommt zunächst ein **Auskunftsanspruch nach Art. 8 Abs. 1** des Bayerischen Daten-

schutzgesetzes. Danach hat der Angezeigte gegen die Gemeinde einen Anspruch auf Auskunft über die Daten des Anzeigeerstatters, wenn sie in einer seine Person betreffenden Datei/Kartei gespeichert werden. Die Auskunftserteilung unterbleibt u.a., soweit durch die Auskunft die **rechtmäßige Aufgabenerfüllung** der speichernden Stelle gefährdet würde oder die personenbezogenen Daten wegen den **überwiegenden berechtigten Interessen einer dritten Person** geheimgehalten werden müssen. Die ordnungsgemäße Aufgabenerfüllung kann z.B. beeinträchtigt werden, wenn der Behörde Gefahren, Mißstände und Verstöße gegen Vorschriften nicht mehr mitgeteilt werden, weil Informanten künftig befürchten müßten, daß ihr Name dem Angezeigten preisgegeben und sie von diesem in ungehöriger Weise zur Rechenschaft gezogen würden.

Nach dem neuen Bayerischen Datenschutzgesetz, das am 1. März 1994 in Kraft treten wird, erstreckt sich der Auskunftsanspruch auch auf Speicherungen in Akten.

2. In einem **Verwaltungsverfahren** hat der Angezeigte außerdem nach Art. 29 Abs. 1 des Bayerischen Verwaltungsverfahrensgesetzes (BayVwVfG) als Beteiligter ein Akteneinsichtsrecht, soweit dies zur Geltendmachung oder Verteidigung seiner **rechtlichen** Interessen **erforderlich** ist. Die Gemeinde ist zur Gestattung der Akteneinsicht nach Art. 29 Abs. 2 BayVwVfG allerdings u.a. nicht verpflichtet, soweit durch sie die **ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigt** oder soweit die Vorgänge nach einem Gesetz oder ihren Wesen nach, namentlich wegen der **berechtigten Interessen der Beteiligten** oder dritter Personen, geheimgehalten werden müssen.

3. In einem **Ordnungswidrigkeitenverfahren** steht dem Angezeigten nach § 147 der Strafprozeßordnung i.V.m. § 46 Abs. 1 des Ordnungswidrigkeitengesetzes nur das Recht auf **Akteneinsicht** zu, das jedoch in der Regel grundsätzlich nur von einem Verteidiger ausgeübt werden kann.

7.9 Aufzeichnung ankommender Telefongespräche

Ein Landratsamt bat mich zu prüfen, ob es zulässig ist, den gesamten Telefonsprechverkehr des Landratsamtes aufzuzeichnen bzw. alternativ oder zusätzlich Gesprächsaufzeichnungen beim Telefonanschluß des Landrats durchzuführen, da Bombendrohungen gegen das Landratsamt und Attentatsdrohungen gegenüber dem Landrat und Beschäftigten eingegangen seien.

Das Staatsministerium des Innern vertritt zur Aufzeichnung von Telefongesprächen, die bei Behörden auflaufen, die folgende Auffassung, die ich teile:

1. Die Aufzeichnung des Inhalts von Telefongesprächen ist nach § 201 des Strafgesetzbuches zu beurteilen. Folgende Fallgruppen sind zu unterscheiden:

   - **Stellen, die Notrufe entgegennehmen**

     Die Aufzeichnung von Telefongesprächen über den Notruf 110 (Polizei) ist nach Art. 31 Abs. 1 Nr. 1, 2 und Art. 38 Abs. 1 des Polizeiaufgabengesetzes zulässig. Im übrigen kann bei Notrufen, die bei der Polizei, der Feuerwehr oder dem Rettungsdienst eingehen, von einer konkludenten Einwilligung der Betroffenen in die Aufzeichnung ausgegangen werden. Es kann geradezu als Aufgabe dieser Stellen angesehen werden, die oft undeutlichen Meldungen aufzuzeichnen, um wirksame Hilfe leisten zu können. Die Tatsache der Aufzeichnung ist hier auch allgemein bekannt.

   - **Besonders gefährdete Stellen**

     Besonders gefährdete Stellen (wie z.B. Flughäfen) dürfen alle Telefongespräche kurzfristig aufzeichnen. In den bekannten Fällen beträgt die Aufzeichnungsdauer 4 Minuten. Nach Ablauf dieser Zeit werden die Aufzeichnungen automatisch gelöscht, es sei denn, der Angerufene drückt bei eingehenden (Bomben-) Drohungen eine besondere „Bedrohungstaste".

     Eine solche Verfahrensweise begegnet im Hinblick auf die Grundsätze zur mutmaßlichen Einwilligung bzw. der Notwehr sowie des rechtfertigenden Notstandes keinen Bedenken.

   - **Besondere Gefährdung im Einzelfall**

     Bei Vorliegen einer besonderen Gefährdung im Einzelfall ist es zulässig, daß auch von sonstigen Behörden nach oben geschilderter Aufzeichnungsmethode (oder einer vergleichbaren Technik) die Telefongespräche kurzfristig aufgezeichnet werden. Das gilt nach meiner Auffassung insbesondere dann, wenn sich Bomben- und Attentatsdrohungen häufen.

2. Eine Aufzeichnung der Gesprächsinhalte von Telefonaten mit Behördenangehörigen bedarf der Mitbestimmung des Personalrats (Art. 75 a Abs. 1 Nr. 1 und Art. 75 Abs. 4 Nr. 8 des Bayerischen Personalvertretungsgesetzes). Soweit die bei der Telefonzentrale eingehenden Gespräche aufgezeichnet werden und die Aufzeichnung beendet wird, sobald das Gespräch weitervermittelt wird, ist noch kein Mitbestimmungsrecht des Personalrats gegeben.

7.10 Bürgerbefragung mit Preisausschreiben

Eine Stadt wollte ihre Bürger befragen, wie diese die Stadt beurteilen, welche Verbesserungen vorgenommen werden sollten und welche Einrichtungen sie vermissen. Dazu sollten die Bürger einen umfangreichen Fragebogen ausfüllen. Um eine möglichst große Beteiligung an

der Fragebogenaktion zu erreichen, war vorgesehen, unter den Teilnehmern eine Gewinnauslosung durchzuführen. Dazu sollten die Teilnehmer Name und Anschrift auf den ausgefüllten Fragebögen mitteilen. Diese sollten bei den Kreditinstituten, bestimmten Geschäften und im Rathaus abgegeben werden.

Bei diesem Verfahren hätten unbefugte Dritte von den mit Namen und Anschrift ausgefüllten Fragebögen Kenntnis nehmen können. Ich habe der Stadt mitgeteilt, daß ich die Bürgerbefragung aus datenschutzrechtlicher Sicht für zulässig halte, wenn folgende Grundsätze beachtet werden:

- Die Bürger, die am Preisausschreiben nicht teilnehmen wollen, müssen den Fragebogen auch anonym abgeben können.
- Die Fragebögen können in einem verschlossenen Umschlag abgegeben werden. Dies gilt insbesondere für die Bürger, die am Preisausschreiben teilnehmen und deshalb ihre Namen und ihre Adresse auf dem Fragebogen angeben. Die Teilnahme sollte möglich sein, ohne daß Dritte die Antworten der Teilnehmer lesen können.
- Der für die Teilnahme am Preisausschreiben vorgesehene Abschnitt mit Namen und Anschrift ist vor der Auswertung vom Fragebogen zu trennen. Auf diese Weise sollte die Antwort so frühzeitig wie möglich anonymisiert werden.
- Die Bürger sind ist auf dem Fragebogen auf ihre Möglichkeiten deutlich hinzuweisen.

8. Einwohnermelde-, Standesamts- sowie Paß- und Ausweiswesen

8.1 Prüfungen

Nachdem in den letzten Jahren der Prüfungsschwerpunkt im Einwohnermeldewesen bei kommunalen Eigenentwicklungen und bei Verfahren kleinerer privater Softwarehersteller lag, habe in diesem Jahr den Einsatz von automatisierten **Einwohnermeldeverfahren größerer Anbieter** überprüft.

Bei den Prüfungen habe ich insbesondere folgende **Mängel** festgestellt:

- Mangelhafte **Zugriffssicherung**

  Die Zugriffssicherung durch **Paßwörter** wurde vernachlässigt (Verwendung von Trivialpaßwörtern, kein Paßwortwechsel). Die datenschutzrechtlichen Anforderungen sind unter Nr. 20.2.2 meines 14. Tätigkeitsberichtes dargestellt.

- Keine **Reduzierung der Datensätze** bei der Meldebehörde der **Nebenwohnung.**

  Die Datensätze von Bürgern, die ihren Wohnstatus von der Haupt- auf die Nebenwohnung verändert haben, wurden nicht auf den zulässigen Umfang reduziert.

  Die Meldebehörde einer Nebenwohnung darf grundsätzlich nur die in Art. 3 Abs. 1 und Abs. 2 Nrn. 6, 7 (nur bei ausländischen Staatsangehörigen) und 11 MeldeG bezeichneten Daten (vgl. Nr. 3.2 Satz 2 VollzBekMeldeG) speichern. Sofern ein Einwohner den Status seiner Wohnung von der Haupt- zur Nebenwohnung ändert, hat die Meldebehörde die gespeicherten Datensätze gemäß Art. 11 Abs. 1 MeldeG auf den für Nebenwohnungen zulässigen Umfang zu reduzieren.

- Keine **Reduzierung der Datensätze** beim **Wegzug** oder **Tod** eines Einwohners

  Bei den überprüften Verfahren war festzustellen, daß nach dem Wegzug oder Tod eines Einwohners die Datensätze nicht auf den nach Art. 11 Abs. 2 Satz 1 MeldeG zulässigen Umfang reduziert wurden.

  Nach dem Wegzug oder Tod eines Einwohners sind die Daten und Hinweise aus dem Hauptregister zu löschen und in reduziertem Umfang in das Nebenregister aufzunehmen (vgl. Art. 11 Abs. 2 MeldeG sowie Nrn. 11.1 Satz 1 und 3.1.2 Satz 2 VollzBekMeldeG). Nur die zur Erstellung von Lohnsteuerkarten erforderlichen Daten nach Art. 3 Abs. 2 Nr. 2 MeldeG dürfen noch bis zum Ablauf des auf den Tod oder Wegzug folgenden Kalenderjahres im Hauptregister gespeichert bleiben (Art. 11 Abs. 2 Satz 1 Halbsatz 2 MeldeG).

- **Speicherung** der Meldedaten **nach Ablauf von 5 Jahren** nach dem Wegzug oder Tod eines Einwohners

  Die Löschung der Daten aus dem Melderegister nach Ablauf von 5 Jahren nach dem Wegzug oder Tod eines Einwohners wurde nicht vollzogen.

  Nach Art. 11 Abs. 3 Satz 1 MeldeG sind die Daten über weggezogene oder verstorbene Bürger nach Ablauf von 5 Jahren aus dem Melderegister (Nebenregister) zu löschen und für die Dauer von 50 Jahren **gesondert** aufzubewahren. Diese Daten sind durch technische und organisatorische Maßnahmen besonders zu sichern. Während der Zeit von 50 Jahren dürfen sie mit Ausnahme der Anschrift und des Sterbetages nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur Aufgabenerfüllung von Sicherheitsbehörden oder für Wahlzwecke unerläßlich ist oder der Betroffene schriftlich eingewilligt hat. Nach Ablauf von 50 Jahren sind diese Daten zu löschen.

- **Speicherung von Paß- und Personalausweisnummern**

  Bei einem Verfahren konnte über eine Auskunftsmaske des Melderegisters weiterhin die Paß- und Personalausweisnummer über den Namen des Ausweisinhabers abgefragt werden. Die Speicherung von Seriennummern deutscher Pässe und Ausweise

im Melderegister ist seit dem 1. September 1991 nicht mehr zulässig (§ 16 Abs. 4 Satz 3 PaßG und § 3 Abs. 4 Satz 3 PAuswG). Das **Paß- und Personalausweisregister** ist gesondert zu führen.

- **Differenzierung zwischen Wahlrechtsausschlüssen**

  In den überprüften Melderegistern wurde größtenteils noch zwischen Wahlrechtsausschlüssen zu Bundestags-, Landtags- und Kommunalwahlen differenziert. Diese Differenzierung ist mit Erlaß des Betreuungsgesetzes entfallen. Die Wahlrechtsausschlüsse sind nun für sämtliche Wahlen identisch. Die Differenzierung zwischen Wahlrechtsausschlüssen zu Bundestags-, Landtags- und Kommunalwahlen ist deshalb aufzuheben.

- **Unzulässige Hinweise zur Wehrpflicht**

  In einem Melderegister wurden im Datenfeld „Wehr-/Zivildienst" folgende Angaben gespeichert: „Wehrüberwachung bis zum 32. Lebensjahr", „keine Wehrüberwachung". Die Speicherung solcher Hinweise ist unzulässig.

  Nach Art. 3 Abs. 2 MeldeG dürfen die Meldebehörden, falls dies zur Mitwirkung bei der Wehr-/Zivildienstüberwachung **erforderlich** ist, die **Tatsache,** daß der Betroffene der Wehr- oder Zivildienstüberwachung unterliegt, speichern. Hierzu genügt die Belegung des Datenfeldes mit der Angabe „Ja" oder „Nein". Die Speicherung dieser Tatsache ist nur erforderlich, soweit der Bürger das 32. Lebensjahr überschritten hat und vom Kreiswehrersatzamt mitgeteilt wurde, daß diese Person noch der Wehrüberwachung unterliegt (§ 29 Abs. 9 Satz 2 WPflG).

  Im übrigen teilt die Meldebehörde zum Zweck der Wehr- und Zivildienstüberwachung dem zuständigen Kreiswehrersatzamt die in § 18 MRRG genannten Daten **aller männlichen Deutschen** zwischen dem vollendeten 18. und 32. Lebensjahr sowie spätere Änderungen dieser Daten mit (§ 24 Abs. 9 WPflG, § 23 Abs. 3 ZDG und § 2 2. BMeldeDUV). Die Speicherung der Tatsache, daß ein Bürger wehr- oder zivildienstpflichtig ist, ist bei diesem Personenkreis daher nicht erforderlich und damit unzulässig. Nicht erforderlich und unzulässig sind auch sonstige Vermerke wie „Zivildienst", „Katastrophenschutz", „Wehrdienstüberwachung bis zum 32. Lebensjahr", „keine Überwachung" usw.

- **Behandlung von Aussiedlern**

  Die 2-Jahresfrist bei der Meldung des Personenkreises nach § 41 WPflG (Aussiedler nach § 1 Abs. 2 Nr. 3 Bundesvertriebenengesetz) wird oft nicht beachtet. Zur Überwachung des Personenkreises empfehle ich den Gemeinden, nach den Verfahrenshinweisen in der Bek. des Staatsministeriums des Innern v. 15. Januar 1991, AllMBl. S. 72 f., vorzugehen. Danach verfügt die Gemeinde als Erfassungsbehörde bei Vorliegen der Voraussetzungen nach § 41 WPflG eine manuelle oder automatische Wiedervorlage **außerhalb des Melderegisters.** Beim Umzug einer Person, die unter § 41 WPflG fällt, ist die Erfassungsbehörde der Zuzugsgemeinde mit dem vorgesehenen Formblatt zu unterrichten (vgl. Nr. 5.2, 5.3 und Anlage zu o.a. Bek.).

- **Keine Anhörung vor Auskunft aus dem Melderegister über Pflegeheimbewohner**

  Pflegeheiminsassen wurden vor Erteilung von Melderegisterauskünften nicht angehört.

  Die Meldebehörden dürfen Daten über Personen, die in Krankenhäusern, Pflegeheimen oder sonstigen Einrichtungen, die der Betreuung pflegebedürftiger oder behinderter Menschen, der Rehabilitation oder der Heimerziehung dienen, aufgenommen wurden, nur übermitteln, wenn sie durch Prüfung im Einzelfall festgestellt haben, daß durch die Übermittlung keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden. Vor Melderegisterauskünften ist der Betroffene zu hören (Art. 28 Abs. 1 Satz 5 und Art. 25 Abs. 4 Satz 4 MeldeG). Die vorherige Anhörung des betroffene Personenkreises ist bei den Meldebehörden sicherzustellen. Auf Nr. 8.2 im 14. Tätigkeitsbericht, S. 65 f., weise ich hin.

- **Keine Wahrung des Adoptionsgeheimnisses**

  Bei einer Meldebehörde wurden nach vollzogener Adoption der frühere Name eines Kindes weiter gespeichert und die Datenweitergabe durch einen Sperrvermerk gesichert. Diese Verfahrensweise entspricht nicht den Vorgaben zur Wahrung des Adoptionsgeheimnisses.

  Bei der Annahme eines Kindes (Adoption) darf im Zusammenhang mit dem neuen Namen weder der vor der Adoption geführte Name noch ein sonstiger Hinweis auf die Adoption im Melderegister gespeichert werden. Bei vollzogener Adoption sind auch die im Adoptionsverfahren veranlaßten Auskunftssperren zu löschen, da diese auf die Adoption hinweisen würden. Nur wenn der Adoptierte zum Zeitpunkt der Adoption bereits volljährig war, ist der frühere Name im Nebenregister zu speichern (Nr. 3.1.5 VollzBekMeldeG).

- **Unzulässige Eingabemöglichkeit für Ausländerdaten**

  In einem Melderegister fand ich das Datum „Wohnungsgeber". Das Datenfeld wurde von der Gemeinde bei Ausländern belegt, um im Falle von Rückfragen deren Wohnungsgeber ermitteln zu können. Das Datenfeld war auf Wunsch der Gemeinde vom Software-Hersteller in das Melderegister aufgenommen worden. Die Speicherung eines solchen „zusätzlichen Datums" ist nicht zulässig.

  Die zulässigerweise im Melderegister zu speichernden Daten ergeben sich abschließend aus Art. 3 Abs.

1 und 2 MeldeG in Verbindung mit dem Datensatz für das Meldewesen (DSMeld). Zusätzliche Angaben wie z.B. „Wohnungsgeber", „Aufenthaltserlaubnis", „Asylbewerber", „Duldung", „Abschiebung" usw. sind in Art. 3 Abs. 1 und 2 MeldeG und im DSMeld nicht vorgesehen und dürfen daher nicht im Melderegister gespeichert werden. Die Speicherung außerhalb des Melderegisters bleibt unberührt.

8.2 Weitergabe von Meldedaten zur Berechnung von Müllgebühren

Um die Müllgebühren in Form einer einwohnerbezogenen Grundgebühr erheben zu können, bat mich ein Landkreis zu prüfen, ob zur Veranlagung der Abfallgebühren die Einwohneradressen aller Gemeinden im Landkreis an das Landratsamt oder an eine andere zentrale Stelle im Landkreis übermittelt werden können.

Die beabsichtigte **regelmäßige** Übermittlung der Einwohneradressen an die Landkreise ist unzulässig. Nach Art. 31 Abs. 4 des Meldegesetzes sind regelmäßige Datenübermittlungen der Meldebehörden an **andere** Behörden oder sonstige öffentliche Stellen nur zulässig, soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlung, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. In der geltenden bayerischen Meldedatenübermittlungsverordnung ist eine regelmäßige Datenübermittlung von Meldedaten für Zwecke der Abfallbeseitigung an die Landratsämter oder Abfallzweckverbände nicht vorgesehen. Gegen eine entsprechende Änderung hätte ich keine Bedenken. Was in kreisfreien Städten möglich und zulässig ist, darf in Landkreisen nicht durch enge Datenschutzvorschriften verhindert werden.

Keine datenschutzrechtlichen Bedenken bestehen gegen die Praxis, die verwaltungsmäßige Abwicklung der Gebührenerhebung vom Landkreis auf die Gemeinden zu übertragen. Die Gemeinden können dann die aktuellen Einwohnermeldedaten bei der Berechnung der einwohnerbezogenen Grundgebühr verwenden, da es zur Datenübermittlung **innerhalb** der Gemeindeverwaltung nach Art. 31 Abs. 7 keiner besonderen Rechtsgrundlage bedarf.

8.3 Weitergabe von Meldedaten an ein Hochschulinstitut zur Erforschung von Leukämie-Erkrankungen bei Kindern

Ein Hochschulinstitut führt derzeit zur Erstellung eines Kinderkrebsregisters Untersuchungen zu den Ursachen von Leukämie bei Kindern und Jugendlichen durch. Dazu ist es erforderlich, über die Einwohnermeldeämter Vergleichs- bzw. Kontrollpersonen zu ermitteln. Zu diesem Zweck übersendet das Hochschulinstitut ausgewählten Gemeinden eine Liste mit Angaben über das Geschlecht und das Geburtsdatum von Kindern ohne deren Namen, zu denen **Vergleichspersonen** gesucht werden sollen. Die Gemeinden entnehmen aus dem Melderegister zu jedem aufgeführten Geburtsdatum den Namen und die Anschrift der Eltern von Kindern, die am gleichen Tag Geburtstag haben oder deren Geburtstag dem Tag am nächsten kommt, und führen diese auf der Liste auf. Die Angabe des Geburtsdatums des betroffenen Kindes ist dabei nicht erforderlich. Anhand der so über die Meldeämter ermittelten Adressen bittet das Hochschulinstitut die Eltern zur freiwilligen Teilnahme an der Studie.

Gegen die geplante Ermittlung von Vergleichs- und Kontrollpersonen über die Einwohnermeldeämter bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Rechtsgrundlage für die Übermittlung des Namens und der Anschrift der betroffenen Eltern ist Art. 31 Abs. 1 Satz 1 Nr. 1 und 5 Meldegesetz. Die Datenübermittlung ist demnach zulässig, da die Elterndaten zur Erstellung des Kinderkrebsregisters benötigt werden.

Ich mache jedoch darauf aufmerksam, daß die Meldebehörde das Hochschulinstitut bei der Übermittlung der Daten zu Forschungszwecken auf den **Zweckbindungsgrundsatz** (Art. 31 Abs. 6 MeldeG) hinzuweisen hat, und daß die Datenübermittlung mit den in Nr. 34.6 Abs. 4 VollzBekMeldeG beschriebenen Auflagen zu versehen ist (Nr. 31.11 Abs. 2 VollzBekMeldeG).

8.4 Melderegisterauskunft an Kreditauskunfteien

Zum Thema Melderegisterauskünfte an Kreditauskunfteien u.ä. habe ich mich bereits im 12. und 14. Tätigkeitsbericht unter Nr. 8.4.5 bzw. 8.3 geäußert. Auch im Berichtszeitraum haben mich zu diesem Themenbereich mehrere Anfragen und Beschwerden erreicht.

Ein Bürger beklagte sich darüber, daß eine Meldebehörde vor Erteilung der Auskunft Rückfragen bei der anfragenden Kreditauskunftei über die Gründe der Anfrage gestellt und dabei auch das Geburtsdatum mitgeteilt habe.

Bei der Mitteilung des Geburtsdatums handelt es sich um eine sog. erweiterte Melderegisterauskunft nach Art. 34 Abs. 2 Nr. 1 MeldeG. Nach dieser Vorschrift darf die Meldebehörde eine erweiterte Melderegisterauskunft nur bei Vorliegen eines „berechtigten Interesses" erteilen. Als berechtigtes Interesse ist jedes von der Rechtsordnung erlaubte, insbesondere auch ein wirtschaftliches Interesse anzusehen. Kreditauskunfteien haben in der Regel ein berechtigtes Interesse an einer erweiterten Auskunft, deren Hintergrund Geschäftsanbahnungen, Kreditentscheidungen usw. sind. Vor Erteilung der Melderegisterauskunft war die Gemeinde verpflichtet, sich über die näheren Umstände des berechtigten Interesses zu erkundigen und im Zweifel Rückfragen bei der Kreditauskunftei anzustellen.

Nachdem die Kreditauskunftei dargelegt hatte, daß sie das Geburtsdatum des Betroffenen benötige, um ihn im Rahmen eines Kreditgeschäfts als zweiten Vorsitzenden eines Vereins zu identifizieren, war die Weitergabe des Geburtsdatums zulässig.

Zum Ausgleich für die Herausgabe dieses zusätzlichen Datums war die Meldebehörde verpflichtet, den Betrof-

fenen über die Auskunftserteilung unverzüglich zu unterrichten, was auch geschehen ist. Das Vorgehen der Meldebehörde war damit nicht zu beanstanden.

8.5 Übermittlung der Adressen der Inhaber von Nebenwohnungen an die Freiwillige Feuerwehr

Eine Gemeinde bat mich zu prüfen, ob die Weitergabe der Anschriften der Inhaber von Nebenwohnungen aus dem Melderegister an die Freiwillige Feuerwehr zur Erlangung von Förderungsbeiträgen zulässig ist.

Bei Auskunftserteilungen an die Freiwillige Feuerwehr ist zu unterscheiden, ob der Empfänger der Daten die Freiwillige Feuerwehr als **gemeindliche Einrichtung** oder die Freiwillige Feuerwehr e.V. als **Verein des privaten Rechts** sein soll.

- **Datenübermittlung an die gemeindliche Einrichtung**

  Die Übermittlung der Adressen der Inhaber von Nebenwohnungen an die gemeindliche Einrichtung Freiwillige Feuerwehr beurteilt sich nach Art. 31 Abs. 7 Satz 1 i.V.m. Art. 31 Abs. 1 Satz 1 MeldeG. Danach wäre die Datenweitergabe zulässig, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit 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 Satz 1 Bayerisches Feuerwehrgesetz). Die Akquisition von Spenden oder Mitgliedsbeiträgen gehört nicht zu den Aufgaben der gemeindlichen Einrichtung Freiwillige Feuerwehr. Die Übermittlung der Adressen der Inhaber von Nebenwohnungen an die Freiwillige Feuerwehr als gemeindliche Einrichtung ist damit unzulässig.

- **Datenübermittlung an den Feuerwehrverein (Freiwillige Feuerwehr e.V.)**

  Im Rahmen der Auskunftserteilung sollten die Anschriften einer Vielzahl namentlich nicht bezeichneter Einwohner (Inhaber von Nebenwohnungen) an den Feuerwehrverein, bei dem es sich nicht um eine gemeindliche Einrichtung handelt, weitergegeben werden. Damit handelte es sich um eine Gruppenauskunft, deren Zulässigkeit sich nach Art. 34 Abs. 3 MeldeG beurteilt. Danach sind Gruppenauskünfte zulässig, soweit sie im öffentlichen Interesse liegen und die Zustimmung der zuständigen Bezirksregierung vorliegt (vgl. Nr. 34.6 VollzBekMeldeG).

  Soweit die Spenden über den Feuerwehrverein der gemeindlichen Einrichtung Freiwillige Feuerwehr zu deren Aufgabenerfüllung zufließen sollen (z.B. zur Anschaffung von technischem Gerät), könnte zwar ein öffentliches Interesse an der Spendengewinnung angenommen werden. Bei der Beurteilung der Zulässigkeit der Datenübermittlung ist jedoch auch die Erforderlichkeit der Datenübermittlung zu berücksichtigen. Da für die Gewinnung von Spenden auch andere Möglichkeiten bestehen (z.B. Zeitungsanzeigen, Postwurfsendungen, Informationsveranstaltungen etc.) ist die Melderegisterauskunft an den Feuerwehrverein zur Gewinnung von Mitgliedern oder Spenden nicht erforderlich. Hinzu kommt, daß durch die Datenübermittlung schutzwürdige Belange der Inhaber von Nebenwohnungen beeinträchtigt würden. Diese haben ein schutzwürdiges Interesse daran, daß die Gemeinde die Tatsache, daß sie Haus- und Grundbesitz in der Gemeinde haben, nicht ohne ihre Einwilligung dem Feuerwehrverein übermittelt und daß sie von persönlich an sie adressierten Spendenbriefen des Feuerwehrvereins unbehelligt bleiben. Bei einer Abwägung der Interessen des Feuerwehrvereins an der Mitglieder- und Spendengewinnung mit den schutzwürdigen Belangen der Inhaber von Nebenwohnungen, keine Beeinträchtigung ihrer Privatsphäre durch Spendenbriefe hinnehmen zu müssen, überwiegen die schutzwürdigen Belange der Inhaber von Nebenwohnungen.

  Die Übermittlung der Adressen der Inhaber von Nebenwohnungen aus dem Melderegister an den Feuerwehrverein wäre deshalb aus datenschutzrechtlichen Gründen ebenfalls unzulässig.

8.6 Automatisierung der Paß- und Personalausweisregister

Auf die Anfrage einer Gemeinde hin prüfte ich, ob gegen die Automatisierung des Paß- und Personalausweisregisters mittels eines Scanners Bedenken bestehen. Durch die Automatisierung sollte die platzaufwendige Aufbewahrung der Originalunterlagen entfallen.

Die Möglichkeit der automatisierten Führung des Paß- und Personalausweisregisters ist in Nr. 21.3 der Allgemeinen Verwaltungsvorschrift zur Durchführung des Paßgesetzes (PaßVwV) und in Nr. 12.2 der Bekanntmachung zum Vollzug des Gesetzes über Personalausweise (VollzBekPAusw) ausdrücklich vorgesehen.

Zu beachten ist jedoch, daß die personenbezogenen Daten im Paß- und Personalausweisregister, zu denen auch das Lichtbild und die Unterschrift des Paß- bzw. Personalausweisinhabers gehören, bis zur Ausstellung eines neuen Passes oder Personalausweises, höchstens aber bis zu fünf Jahren nach dem Ablauf der Gültigkeit des Ausweispapieres, auf das sie sich beziehen, zu speichern sind (§ 21 Abs. 4 Paßgesetz und § 2 a Abs. 3 Gesetz über Personalausweise). Zweck dieser Regelung ist, daß das Register auch die Identitätsfeststellung von Personen ermöglichen muß (§ 2 a Abs. 2 Nr. 2 Gesetz über Personalausweise). Um diesen Zweck erfüllen zu können, müssen die Lichtbilder in brauchbarer Qualität archiviert werden. Die Reproduktion eines mikroverfilmten oder eines mittels Scanner gespeicherten Lichtbildes war bisher aus technischen Gründen für Identifizierungszwecke unbrauchbar. Wegen der in den letzten Jahren

wesentlich verbesserten technischen Möglichkeiten zur Speicherung von Bildern kann künftig u. U. auf eine Aufbewahrung der Originalanträge mit den Lichtbildern verzichtet werden. Voraussetzung hierzu ist jedoch eine Rekonstruierbarkeit des Paßfotos, die in ihrer Qualität dem Originalfoto gleichkommt. Ob diese Voraussetzung vorliegt, muß im Einzelfall von der Paß- und Ausweisbehörde unter Beteiligung der Aufsichtsbehörden entschieden werden.

8.7 Weitergabe von Meldedaten zur Wahlwerbung

Im Berichtszeitraum erreichten mich wieder zahlreiche Anfragen und Beschwerden von Bürgern, deren Adressen von Meldebehörden zur Wahlwerbung an politische Parteien und Wählergruppen weitergegeben wurden.

Die Weitergabe des Grunddatensatzes (Vor- und Zuname, akademischer Grad und Adresse) von Wahlberechtigten an politische Parteien und Wählergruppen ist im Zusammenhang mit allgemeinen Wahlen innerhalb von 6 Monaten vor der Stimmabgabe zulässig, sofern der Bürger der Datenweitergabe nicht widersprochen hat (Art. 35 Abs. 1 MeldeG). Die Auskunft kann sich auf bestimmte Gruppen von Wahlberechtigten beschränken, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Die Geburtstage der Wahlberechtigten dürfen dabei jedoch nicht mitgeteilt werden. Die Zusammensetzung der Daten von Wahlberechtigten nach anderen Suchkriterien (z.B. „alle Neubürger") ist unzulässig. Auf die in Nr. 9.3 des 11. Tätigkeitsberichts, S. 33, veröffentlichten Entscheidungshilfen für die Meldebehörden weise ich hin.

Auch wenn seit Inkrafttreten der Neufassung des Meldegesetzes am 1.4.1983 bei der Anmeldung eines Zu- oder Umzugs auf das Widerspruchsrecht nach Art. 35 Abs. 1 Satz 3 MeldeG hinzuweisen ist, scheint die Möglichkeit des Widerspruchs bei vielen Bürgern doch weitgehend unbekannt zu sein. Im Hinblick auf das bevorstehende Wahljahr rege ich daher an, die Bürger rechtzeitig in ortsüblicher Weise (z.B. im Mitteilungsblatt der Gemeinde) auf ihr Widerspruchsrecht hinzuweisen.

8.8 Regelmäßige Übermittlung von Einwohnermeldedaten an die GEZ für den Rundfunkgebühreneinzug

Im 14. Tätigkeitsbericht (Nr. 19.5, Seiten 83 und 84) hatte ich gegen die regelmäßige Übermittlung wenig sensibler Meldedaten an die Rundfunkanstalten bzw. an ihre Gebühreneinzugszentrale (GEZ) keine Bedenken geäußert.

Die **Ministerpräsidenten der Länder** haben die Innenministerkonferenz gebeten, ausgehend von den bereits bestehenden Regelungen in Hessen und Nordrhein-Westfalen einen Musterentwurf für eine Vorschrift der Meldedatenübermittlungsverordnungen der Länder zu erarbeiten, der Maßnahmen der Rundfunkanstalten für einen Gebühreneinzug im Sinne der Gebührengerechtigkeit erleichtert.

Der **Unterausschuß** „EDV im Einwohnerwesen" des Arbeitskreises II der Innenministerkonferenz hat inzwischen einen Musterentwurf vorgelegt, der den Anforderungen entspricht, unter denen ich im 14. Tätigkeitsbericht eine regelmäßige Datenübermittlung von den Einwohnermeldeämtern an die GEZ aus datenschutzrechtlicher Sicht für zulässig angesehen habe.

Mit dem Thema hat sich am 26./27. Oktober 1993 auch die **Konferenz der Datenschutzbeauftragten** des Bundes und der Länder befaßt. Die Mehrheit der Datenschutzbeauftragten lehnt nach wie vor eine regelmäßige Weitergabe von Einwohnerdaten an die GEZ mit der Begründung ab, die Datenübermittlung könnte zu einem bundesweiten Melderegister der Volljährigen führen und gegen das Verhältnismäßigkeitsprinzip verstoßen.

Die Annahme, es könnte ein bundesweites Melderegister entstehen, ist schon deshalb völlig abwegig, weil die gemeldeten Daten nach Abgleich mit dem Bestand und Auswertung gelöscht werden. Der Bestand der gemeldeten Rundfunkteilnehmer stellt in keinem Fall ein umfassendes Melderegister dar, weil er nur die Gebührenzahler, nicht aber die Familienmitglieder umfaßt. Die vorgeschlagene Methode der regelmäßigen Übermittlung der Umzüge und Todesfälle stellt die einzige **sinnvolle und praktikable Methode zur Feststellung der gebührenpflichtigen, aber nicht gebührenzahlenden Schwarzhörer und Schwarzseher** dar und ist daher nicht unverhältnismäßig. Die regelmäßige Datenübermittlung dient im Gegenteil durch Verminderung von Einnahmeausfällen durch Schwarzhörer und Schwarzseher in dreistelliger Millionenhöhe der Gebührengerechtigkeit und Lastengleichheit. Sie liegt im Interesse der gesetzestreuen Rundfunkteilnehmer, damit diese wegen der Schwarzhörer und Schwarzseher nicht höhere Gebühren zahlen müssen.

9. Ausländerwesen

9.1 Änderung des Asylverfahrensgesetzes

Im 14. Tätigkeitsbericht habe ich über die Regelung der erkennungsdienstlichen Behandlung der Asylbewerber im Asylverfahrensgesetz vom 26. Juni 1992 berichtet. Dieses Gesetz wurde inzwischen erneut geändert. Es enthält in der seit dem 01. Juli 1993 geltenden Fassung zur Verhinderung von Mißbräuchen eine spezialgesetzliche Bestimmung, mit der ein **erweiterter Informationsaustausch** zwischen öffentlichen Stellen (insbesondere Sozialversicherungsträgern, Sozialämtern, Ausländerbehörden, Gesundheitsämtern, Strafverfolgungsorganen) ermöglicht wird. Nach dem neugefaßten § 8 Abs. 3 Asylverfahrensgesetz dürfen die nach diesem Gesetz erhobenen Daten u.a. auch für Maßnahmen der Strafverfolgung und auf Ersuchen zur Verfolgung von Ordnungswidrigkeiten den damit betrauten öffentlichen Stellen, soweit es

zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist, übermittelt und von diesen dafür verarbeitet und genutzt werden. Eine Datenübermittlung an die zuständigen Behörden ist außerdem zulässig, soweit dies für die Aufdeckung und Verfolgung von unberechtigtem Bezug von Leistungen nach dem Bundessozialhilfegesetz und dem Asylbewerberleistungsgesetz, für Leistungen der Kranken- und Unfallversicherungsträger oder von Arbeitslosengeld oder Arbeitslosenhilfe erforderlich ist und wenn **tatsächliche Anhaltspunkte** für einen unberechtigten Bezug vorliegen.

Die Übermittlung personenbezogener Daten von Asylbewerbern zwischen den beteiligten Stellen ist zur Verhinderung des unberechtigten Leistungsbezugs bei Asylantragstellung unter verschiedenen Identitätsangaben und zur Kriminalitätsbekämpfung angesichts des bekanntgewordenen Ausmaßes der Mißbräuche dringend erforderlich. Ich habe aus datenschutzrechtlicher Sicht daher keine Bedenken gegen die Datenübermittlung.

10. Steuerverwaltung

10.1 Datenschutzvorschriften in der Steuerverwaltung

Seit mehreren Jahren werden von den Finanzministerien des Bundes und der Länder Überlegungen zur Novellierung der Abgabenordnung (AO) angestellt. Dabei sollen neben Vorschriften für das Besteuerungsverfahren und das außergerichtliche Rechtsbehelfsverfahren auch Bestimmungen mit Datenschutzbezug, in der Hauptsache Datenübermittlungen durch Steuerbehörden, geändert werden.

Um so bedauerlicher finde ich Überlegungen im Bundesministerium der Finanzen, eine Novellierung der datenschutzrechtlichen Bestimmungen in der Abgabenordnung wegen Meinungsverschiedenheiten in der Koalition vorerst zurückzustellen.

Ich habe gegenüber dem Staatsministerium der Finanzen darauf hingewiesen, daß insbesondere in folgenden Punkten nach wie vor Handlungsbedarf besteht:

- **Nutzung von Grundsteuer-Adreßdaten durch die Gemeinden für andere öffentliche Aufgaben**

  Die Nutzung aktueller Anschriften, die als nicht besonders schutzwürdige Daten einzustufen sind, liegt nicht zuletzt im Sinne einer unbürokratischen Verwaltung. Nach § 31 Abs. 3 der augenblicklichen Entwurfsfassung wäre die Verwertung der beim gemeindlichen Steueramt vorhandenen aktuellen Adressen der Grundstückseigentümer für die Erhebung und Verwaltung anderer Abgaben sowie zur **Erfüllung sonstiger öffentlicher Aufgaben** zulässig. Diese Regelung würde den Bedürfnissen der Praxis gerecht. Es würde bei den Gemeinden auf Unverständnis stoßen, wenn sie gezwungen wären, kosten- und zeitintensiv ein weiteres Adreßregister aufzubauen, obwohl ein solches im gemeindlichen Steueramt bereits vorhanden ist.

  In diesem Zusammenhang verweise ich auch auf meine Ausführungen im 13. Tätigkeitsbericht (Seite 51, Nr. 10.1).

- Schaffung einer **Rechtsgrundlage für eine automatisiert geführte bundesweite Fahndungsdatei,** die u.a. Auskunft über bereits durchgeführte Steuerfahndungsprüfungen bzw. eingeleitete Bußgeld- und Strafverfahren geben soll.

  Zweck und Umfang der beabsichtigten Fahndungsdatei gebieten es, den Verwendungszweck, die zugelassenen Datenarten, den betroffenen Personenkreis, die Datenempfänger und die Speicherungsdauer gesetzlich festzulegen.

  Ich habe gegenüber dem Finanzministerium die Auffassung vertreten, daß ohne gesetzliche Regelung die Fahndungsdatei nicht geführt werden darf, auch wenn ich deren Notwendigkeit grundsätzlich nicht in Zweifel ziehe. Der vom Bundesverfassungsgericht eingeräumte Übergangsbonus legitimiert nicht die Einrichtung völlig neuer Dateien, bei denen im Hinblick auf den Grundsatz der Normenklarheit ein dringendes Regelungsbedürfnis besteht.

10.2 Prüfung bei einem Finanzamt

Gegenstand der Kontrolle eines Finanzamtes waren Dateien, Karteien, Erhebungsvordrucke und ausgewählte Aktenunterlagen aus verschiedenen Arbeitsgebieten. Kontrollzweck bei der Überprüfung von Steuerakten war die Feststellung von Datenübermittlungen aus Dateien.

Bei der Prüfung waren **nur geringe Mängel** festzustellen:

1. **Unzulässige Angaben im Geschäftsverteilungsplan**

   Zur Prüfungsvorbereitung hat das Finanzamt seinen Geschäftsverteilungsplan zur Verfügung gestellt. Dieser war aufgrund der Vorgaben der Oberfinanzdirektion gefertigt. Der Geschäftsverteilungsplan ist keine nur amtsinterne Unterlage, sondern wird bei Bedarf auch anderen Dienststellen überlassen.

   Der Geschäftsverteilungsplan des geprüften Finanzamts enthält in einem **nachrichtlichen Teil** personenbezogene Angaben von Amtsangehörigen, die für einen ordnungsgemäßen Geschäftsgang nicht erforderlich sind und deren Bekanntgabe an andere Amtsangehörige sowie bei Weitergabe des Geschäftsverteilungsplanes an Außenstehende oder andere Behörden schutzwürdige Belange der betroffenen Personen verletzen könnte. Dies gilt für die namentliche Nennung der Dauerabwesenden, insbesondere der Dauerkranken einschließlich des Datums des Beginns und der voraussichtlichen Dauer der Krankheit, der in Mutterschutz befindlichen Bediensteten, der vom

Dienst enthobenen Beschäftigten sowie für die Angabe des Grundes von Freistellungen und die Auflistung der Beurlaubten und Teilzeitbeschäftigten, getrennt nach Art. 80 a bzw. Art. 86 a BayBG.

Ich habe gebeten, die Vorgaben zu Inhalt und Umfang des Geschäftsverteilungsplanes zu überprüfen.

2. **Fehlende Angabe der Rechtsgrundlage auf Erhebungsvordrucken**

Auf den verwendeten Erhebungsvordrucken fehlte teilweise der in Art. 16 Abs. 2 BayDSG vorgeschriebene Hinweis auf die Rechtsgrundlage der Datenerhebung bzw. auf die Freiwilligkeit der Angaben.

Ich habe die Überarbeitung dieser Vordrucke gefordert.

3. **Überschreitung der Aufbewahrungsfristen**

In der Bußgeld- und Strafsachenstelle werden eine Namenskartei, eine Überwachungsliste für Strafverfahren und eine Bußgeldliste geführt. Diese Unterlagen werden bisher 30 Jahre nach Abschluß des Verfahrens vernichtet.

Gemäß Nr. 4.5.2 und Nr. 4.5.3 der vorläufigen Bestimmungen zur Aufbewahrung und Aussonderung von Schriftgut bei den Finanzämtern sind diese Unterlagen jedoch nach 10 Jahren – datenschutzgerecht – zu vernichten.

Ich habe gebeten, entsprechend diesen Bestimmungen zu verfahren.

4. **Problematische Datenübermittlungen des Finanzamts an Dritte**

Bei der Überprüfung von **Vordrucken** und der stichprobenweisen Aktendurchsicht ergaben sich folgende Feststellungen:

4.1 **Datenübermittlungen an die Gewerbebehörden**

In gravierenden Einzelfällen werden die Gewerbebehörden über die steuerliche Unzuverlässigkeit eines Steuerpflichtigen unterrichtet mit der Bitte, ein Gewerbeuntersagungsverfahren einzuleiten. Die Mitteilung geschieht formlos unter Angabe der Steuerrückstände des Steuerpflichtigen. Einer Mitteilung rückständiger betrieblicher Steuern an die Gewerbebehörde steht nach herrschender Meinung das Steuergeheimnis nicht entgegen (§ 30 Abs. 4 Nr. 5 AO – zwingendes öffentliches Interesse). Die Angabe der Höhe der Steuerrückstände ist für die Entscheidung der Gewerbebehörden erforderlich. Es dürfen in der Regel allerdings nur solche Steuerrückstände mitgeteilt werden, die mit dem Gewerbe in ursächlichem Zusammenhang stehen. Diesen Zusammenhang sieht der BFH bei erheblichen Rückständen an Lohn- und Umsatzsteuer. Bei Personensteuern (z.B. Einkommensteuer) besteht dieser Zusammenhang nur, wenn durch die steuerlichen Unregelmäßigkeiten besondere Vorteile im Wettbewerb erlangt werden.

Gemäß Anlage 1, Nr. 1.16 der Neuregelung des Zeichnungsrechts in den Finanzämtern (ZeiReFA) unterliegen Anträge auf Gewerbeuntersagung dem Zeichnungsvorbehalt des Sachgebietsleiters.

Wegen der Schwere des mit der Übermittlung an die Gewerbebehörde verbundenen Eingriffs in das Persönlichkeitsrecht des Betroffenen und im Interesse der Gleichbehandlung der Steuerpflichtigen eines Amtsbezirks sollte hier wohl eher ein **Zeichnungsvorbehalt des Vorstehers** vorgesehen werden.

Das Staatsministerium hat zugesichert, das Zeichnungsrecht entsprechend zu ändern.

4.2 **Zu weitreichende Datenübermittlungen in der Vollstreckung**

Bei der Vollstreckung in bewegliche Sachen hat der Vollziehungsbeamte dem Schuldner bzw. Dritten gegenüber den Vollstreckungsauftrag vorzuzeigen (§ 285 Abs. 2 AO). Dieser enthält aufgrund der Regelung des § 260 AO eine detaillierte Aufgliederung der beizutreibenden Geldbeträge.

Bei der Pfändung von Sachen, die sich im Gewahrsam eines Dritten befinden, kann dieser somit genau erkennen, welche Steuern, in welcher Höhe und für welchen Zeitraum der Vollstreckungsschuldner schuldet. Der Dritte ist nicht gehindert, diese Daten anderen Personen mitzuteilen. Diese weitreichende Offenbarung personenbezogener Daten, die auch vom Staatsministerium nicht bestritten wird, erscheint sachlich nicht begründet.

Zwar ist die Offenbarung nach §§ 260, 285 Abs. 2, 30 Abs. 4 Nr. 2 AO zulässig. Trotzdem erscheint eine Änderung geboten, um die Offenbarung von Steuerdaten gegenüber Dritten auf das erforderliche Maß zu beschränken. Sinn der Vorschrift des § 260 AO ist, die Interessen des Vollstreckungsschuldners zu schützen. Nur für ihn ist eine Aufgliederung der Schuld nach einzelnen Steuerarten und Zeiträumen erforderlich.

Eine Gesetzesänderung im Zuge der augenblicklichen Novellierung der Abgabenordnung wird vom Staatsministerium der Finanzen nicht unterstützt. Im übrigen kann das Problem auch durch Änderung des verwendeten Vordrucks gelöst werden. Dieser sollte so geändert werden, daß Dritte die Einzelheiten der Schuld nicht erfahren.

Ich werde das Staatsministerium nochmals um Änderung des Formulars bitten.

10.3 Kontrollmitteilungen an das Finanzamt

Zur Kontrolle der Versteuerung von Einnahmen aus öffentlichen Kassen übersandten öffentliche Stellen an die Finanzämter Kontrollmitteilungen über die an Steuerbürger getätigten Zahlungen. Für diese Kontrollmitteilungen gab es bisher keine Rechtsgrundlage (12. Tätigkeitsbericht, Seite 39, Nr. 9.2).

Von der in § 93 a Abgabenordnung enthaltenen Ermächtigung, durch Rechtsverordnung Behörden und öffentlich-rechtliche Anstalten zur Abgabe solcher Kontrollmitteilungen zu verpflichten, hat der Bundesfinanzminister nunmehr Gebrauch gemacht. Die Angabe der **Betragshöhe** in der Mitteilung an das Finanzamt ist bei Zahlungen von Behörden und öffentlich-rechtlichen Rundfunkanstalten entsprechend dem Wortlaut der Ermächtigungsgrundlage nicht vorgesehen. Eine Mitteilung soll auch nur erfolgen, soweit die an denselben Empfänger geleisteten Zahlungen im Kalenderjahr mehr als 3000.- DM betragen haben.

10.4 Zusätze in der Zustellanschrift von Steuerbescheiden

Mehrere Eingaben befaßten sich mit der Verwendung von **Zusätzen in der Zustellanschrift** von Steuerbescheiden. So wurde einem Steuerpflichtigen ein Erbschaftsteuerbescheid im Fensterkuvert mit dem Zusatz „als Rechtsnachfolger für ..." übersandt.

Einem anderen Steuerpflichtigen wurde ein Schreiben der finanzamtlichen Vollstreckungsstelle unter Hinzufügung des Namens einer in Konkurs gefallenen und bereits liquidierten Handelsgesellschaft, an der der Steuerpflichtige beteiligt war, zugestellt.

Beide Petenten sahen sich durch die genannten Zusätze in ihrem Persönlichkeitsrecht verletzt.

Die Bekanntgabe von steuerlichen Verwaltungsakten richtet sich nach § 122 Abgabenordnung (AO). Danach ist ein Verwaltungsakt demjenigen Beteiligten bekanntzugeben, für den er bestimmt ist oder der von ihm betroffen wird. Dabei ist zu unterscheiden, an wen sich der Verwaltungsakt richtet (Steuerschuldner) und wem er bekanntgegeben werden soll (Adressat).

Bei Steuerfestsetzungen ist in der Regel Steuerschuldner und Adressat identisch. Als Adressat kommen jedoch auch Dritte in Betracht, wenn sie für den Steuerschuldner steuerliche Pflichten zu erfüllen haben. Dabei handelt es sich in erster Linie um Fälle, in denen die Bekanntgabe an den Steuerschuldner nicht möglich oder nicht zulässig ist.

Für die Gesamtrechtsnachfolge gilt, daß die Steuerschulden des Rechtsvorgängers auf den Rechtsnachfolger übergehen.

Bei der Liquidation einer Personengesellschaft ist zwischen der gesellschaftlichen und der steuerlichen Liquidation zu unterscheiden. Letztere ist erst gegeben, wenn alle Rechtsbeziehungen zwischen Gesellschaft und Finanzamt unter den Gesellschaftern beseitigt sind.

In beiden genannten Fällen erfolgten die Zusätze zu Recht. Um die inhaltliche Bestimmtheit der Bescheide zu gewährleisten (§ 119 Abs. 1 AO) genügt es aber, den Zusatz jeweils im Bescheidkopf und nicht im Adreßfeld anzubringen.

Die von mir zur Stellungnahme aufgeforderten Finanzämter haben zugesichert, künftig entsprechend zu verfahren.

10.5 Übermittlung von Grundsteuerdaten an Kirchensteuerämter

Eine Gemeinde hat mich um Stellungnahme gebeten, wie mit Anfragen eines Kirchensteueramtes zu verfahren ist, in denen nach den Eigentümern bestimmter land- und forstwirtschaftlicher Grundstücke und dem jeweiligen Grundsteuermeßbetrag gefragt wird.

Bei den Anfragen des Kirchensteueramtes handelt es sich um Anfragen an das **Grundsteueramt der Gemeinde.** Die Grundsteuermeßbeträge unterliegen als Besteuerungsgrundlagen dem Steuergeheimnis (§ 30 Abgabenordnung – AO). Die Offenbarung von Informationen, die dem Steuergeheimnis unterliegen, richtet sich in vorliegendem Fall nach § 31 Abs. 1 AO. Danach sind die Finanzbehörden berechtigt, Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge u.a. an Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, zur Festsetzung von Abgaben mitzuteilen. Für die Datenübermittlung aus dem Bereich der gemeindlichen Steuern (Art. 13 KAG) gelten die Bestimmungen der AO entsprechend (§ 1 Abs. 2 Nr. 1 AO).

Soweit öffentlich-rechtliche Religionsgemeinschaften **Kirchengrundsteuern** erheben, dürfen ihnen somit von den Gemeinden die Grundsteuermeßbeträge derjenigen Grundstückseigentümer mitgeteilt werden, die dieser Religionsgemeinschaft angehören.

Das Grundsteueramt ist im Wege der Amtshilfe verpflichtet, dem Kirchensteueramt Auskunft zu erteilen (§§ 111 ff. AO i.V.m. Art. 16 Abs. 5 Kirchensteuergesetz (KiStG)).

Nach Art. 16 Abs. 5 KiStG ist die Grundsteuerstelle der Gemeinde verpflichtet, dem Kirchensteueramt die erforderlichen Unterlagen zur Festsetzung der Kirchengrundsteuer zur Verfügung zu stellen. Hierzu übermittelt die Gemeinde auch die Grundsteuerhebelisten mit den Angehörigen der anfordernden Kirche oder Religionsgemeinschaft an die Kirchengrundsteuerstelle. Im vorliegenden Fall handelt es sich nur um eine Auskunft im Einzelfall, die sich auf ein bestimmtes Grundstück bezieht. Falls der neue Eigentümer der anfordernden Religionsgemeinschaft angehört, muß die Auskunft im Einzelfall auch über die Bezeichnung des Grundstückes, als Minus zur Übermittlung von Grundsteuerhebelisten mit sämtlichen Angehörigen einer Religionsgemeinschaft, zulässig sein.

Zur Auskunftserteilung benötigen die Grundsteuerstellen den Namen, die Anschrift, das Geburtsdatum und die Konfession des Betroffenen. Soweit diese Daten nicht bereits bei der Grundsteuerstelle bekannt sind, besteht die Möglichkeit, diese von der Meldebehörde zu erheben. Die Zulässigkeit einer solchen Datenübermittlung aus dem Melderegister innerhalb der Gemeindeverwal-

tung beurteilt sich nach Art. 31 Abs. 7 Satz 1 Meldegesetz (MeldeG). Danach ist die Übermittlung des Vor- und Familiennamens, der Anschrift und der Religionszugehörigkeit an das gemeindliche Steueramt zulässig, da diese Daten dort zur Auskunftserteilung und damit zur Aufgabenerfüllung nach §§ 111 ff. AO und Art. 16 Abs. 5 KiStG erforderlich sind.

10.6 Datenübermittlung der Finanzämter an die Kirchensteuerämter bei glaubensverschiedenen Ehen

Immer wieder wenden sich Bürger bei glaubensverschiedenen Ehen wegen des Umfangs der Datenübermittlung der Finanzämter an die Kirchensteuerämter bei Zusammenveranlagung an mich. Diejenigen Ehegatten, die **keiner** umlageerhebenden Religionsgemeinschaft angehören, sehen durch die **Übermittlung der Höhe ihrer Einkünfte an die Religionsgemeinschaft ihres Ehegatten** ihr informationelles Selbstbestimmungsrecht verletzt.

Die Übermittlung der Höhe des Einkommens des keiner umlageerhebenden Religionsgemeinschaft angehörenden Ehegatten ist nur bei dem in Bayern praktizierten Verfahren zur Berechnung der Kirchensteuer des der umlageerhebenden Religionsgemeinschaft angehörenden Ehegatten erforderlich. Im Gegensatz zu den anderen Ländern wird in Bayern die für die Kirchensteuer relevante Bemessungsgrundlage des kirchensteuerpflichtigen Ehegatten nicht vom Finanzamt sondern vom Kirchensteueramt auf der Grundlage der nach dem Kirchensteuergesetz maßgeblichen Steuerdaten errechnet. Die Berechnung der Kirchensteuer bei glaubensverschiedenen Ehen läuft in folgenden Schritten ab:

Zur Berechnung der Kirchensteuer des Ehegatten, der einer Kirchensteuer erhebenden Religionsgemeinschaft angehört, ist zunächst der auf diesen Ehegatten entfallende relevante Betrag der gemeinsam festgesetzten Einkommensteuer zu errechnen. Nach Art. 9 Abs. 2 Kirchensteuergesetz (KiStG) ist hier die gemeinsame Einkommensteuer im Verhältnis der Einkommensteuerbeträge aufzuteilen, die sich bei Anwendung der für die getrennte Veranlagung geltenden Einkommensteuertabelle (Grundtabelle) auf die Einkünfte eines jeden Ehegatten ergeben würden. Zur Durchführung dieses Rechenvorgangs teilt derzeit das Finanzamt dem Kirchensteueramt die festgesetzte gemeinsame Einkommensteuer, die Anzahl der berücksichtigungsfähigen Kinder, die Gesamtsumme der Einkünfte und die Summe der Einkünfte des der Religionsgemeinschaft angehörenden Ehegatten mit. Durch Differenzbildung ergeben sich somit die Einkünfte des anderen Ehegatten. Das **Kirchensteueramt errechnet** daraus den Anteil des Kirchenmitglieds an der gemeinsamen Einkommensteuer und setzt hieraus die Kirchensteuer fest.

Die Übermittlung dieser Besteuerungsmerkmale stützt sich derzeit auf § 31 Abs. 1 Abgabenordnung (AO) und Art. 9 Abs. 2 KiStG.

Der Bundesfinanzhof hat zwar mit Beschluß vom 22. Oktober 1991 die Klage eines keiner Religionsgemeinschaft angehörenden Bürgers wegen der Übermittlung seiner Einkunftsdaten an das Kirchensteueramt abgewiesen.

Dennoch halte ich das **augenblicklich praktizierte Verfahren für verbesserungsbedürftig.** Es orientiert sich nicht an dem Grundsatz des geringstmöglichen Eingriffs in das informationelle Selbstbestimmungsrecht des Betroffenen. Das Einkommen des nicht einer Kirche angehörenden Ehegatten wird der Kirche nur deshalb bekannt, weil die Berechnung der relevanten **Einkommensteuer** des Kirchenmitglieds nicht vom staatlichen Finanzamt sondern vom Kirchensteueramt vorgenommen wird.

Weder im Einkommensteuer- noch im Kirchensteuergesetz ist bestimmt, daß der bereits beschriebene **Rechenvorgang** zur Anteilsbestimmung an der gemeinsamen Einkommensteuer vom **Finanzamt** durchzuführen ist. Das Kirchensteuergesetz legt aber auch nicht fest, daß er beim **Kirchensteueramt** ablaufen muß. Eindeutig rechtlich festgelegt ist nur, daß die Festsetzung der Kirchensteuer vom Kirchensteueramt durchzuführen ist. Von einer Festsetzung durch das Kirchensteueramt kann beim vorgenannten Rechenvorgang nicht gesprochen werden. Die Errechnung des Verhältnissatzes des Steueranteils des Kirchenmitglieds besteht nur aus der Anwendung der Grundtabelle und eines einfachen Viersatzes. Auch bei der Einkommensteuer wird unter „Festsetzung" die verbindliche Festlegung der Steuerschuld verstanden. Die Wiedergabe der Besteuerungsgrundlagen aus dem Einkommensteuerbescheid und die nötigen Rechenvorgänge enthalten keine Festsetzung. Die Festsetzung der Kirchensteuer im eigentlichen Sinne erfolgt, wie bei nichtglaubensverschiedenen Ehen, durch Anwendung des Kirchensteuersatzes auf die Bemessungsgrundlage „Einkommensteuer" oder in vorliegendem Fall „fiktive Einkommensteuer".

Würde der in Art. 9 Abs. 2 Nr. 2 Satz 2 KiStG beschriebene Rechenvorgang von den Finanzämtern durchgeführt und dem Kirchensteueramt nur der Betrag der anteiligen Einkommensteuer des Kirchenmitglieds bekanntgegeben, würde dies mithin nicht gegen das Festsetzungsrecht des Kirchensteueramts verstoßen. Die Berechnung durch das Finanzamt wäre nach dem geltenden Steuerrecht mithin nicht unzulässig. Sie wird im übrigen auch **in anderen Bundesländern von den Finanzämtern durchgeführt.** Allerdings ordnen und verwalten die Religionsgemeinschaften ihre Angelegenheiten selbständig nach Maßgabe der landesrechtlichen Bestimmungen (Art. 140 Grundgesetz, Art. 137 Weimarer Reichsverfassung).

Zur Begrenzung des Eingriffs in das informationelle Selbstbestimmungsrecht des nicht der Kirche angehörenden Ehegatten wäre auch **in Bayern eine Verlagerung des Rechenvorgangs auf die Finanzämter angezeigt.** Statt der Darstellung der Berechnungsgrundlagen im

Kirchensteuerbescheid müßten diese in einem nachrichtlichen Teil des Einkommensteuerbescheids ausgewiesen werden. Adressat von Einsprüchen bliebe, wie bisher (Art. 18 Abs. 5 KiStG), das Kirchensteueramt.

Die Ehegatten könnten in diesen Fällen **selbst entscheiden,** ob die Höhe der Einkünfte des glaubensverschiedenen Ehegatten gegenüber dem Kirchensteueramt offenbart werden soll um eine Änderung des Kirchensteuerbescheids zu betreiben.

Auf die Finanzverwaltung entfiele **mit Ausnahme des einmaligen Programmieraufwandes keine zusätzliche Arbeitsbelastung.**

Ich habe bereits Stellungnahmen der beiden großen umlageerhebenden Religionsgemeinschaften und des Staatsministeriums der Finanzen eingeholt. Die Kirchen berufen sich bei ihrer Ablehnung auf ihr grundgesetzlich zugestandenes Selbstverwaltungsrecht. Insbesondere betrachten sie den durchzuführenden Rechenvorgang als Teil des ausschließlich ihnen zustehenden Kirchensteuerfestsetzungsverfahrens. Das Staatsministerium befürchtet Mehrarbeit für die Finanzverwaltung und eine geringere Transparenz für den Steuerbürger.

Ich teile diese Auffassung aus den genannten Gründen nicht.

10.7 Kuvertierung von Realsteuerbescheiden durch eine Privatfirma

Eine Gemeinde hat mich gefragt, ob in der Vergabe der maschinellen Kuvertierung von Realsteuerbescheiden an eine Privatfirma ein Verstoß gegen das Steuergeheimnis vorliegt.

Die Einschaltung der Privatfirma war erforderlich geworden, nachdem aufgrund einer Erhöhung der Hebesätze eine größere Anzahl von Grund- und Gewerbesteuerbescheiden zu versenden war, was die Kapazität des gemeindlichen Steueramtes überstieg.

Ich habe in Übereinstimmung mit dem Staatsministerium der Finanzen die Auffassung vertreten, daß das **Falten** und **Kuvertieren** von Steuerbescheiden durch eine Privatfirma, zumindest im weitesten Sinne, der Durchführung eines Steuerverfahrens dient und deshalb ein Offenbarungstatbestand i.S. des § 30 Abs. 4 Nr. 1 Abgabenordnung (AO) gegeben ist.

Die Beschäftigten des Privatunternehmens müssen allerdings nach § 1 des Verpflichtungsgesetzes zur gewissenhaften Erfüllung der Obliegenheiten verpflichtet und auf die strafrechtlichen Konsequenzen von Pflichtverletzungen hingewiesen werden. Der Schutz des Steuergeheimnisses durch § 30 AO, § 355 StGB bleibt insoweit erhalten.

Ich habe außerdem empfohlen, den ordnungsgemäßen Ablauf der durchzuführenden Arbeiten durch einen Bediensteten der Stadt überwachen zu lassen.

Soweit auch die **Versendung** der Bescheide einer Privatfirma übertragen wird, halte ich eine vertragliche Verpflichtung des Unternehmens dergestalt für erforderlich, daß Versandlisten, Versendungsnachweise oder sonstige Unterlagen mit personenbezogenen Daten über Steuerpflichtige nach Abschluß der Aktion an das gemeindliche Steueramt auszuhändigen sind. Eine Verwertung der bekanntgewordenen Verhältnisse außerhalb des in § 30 Abs. 4 Nr. 1 AO genannten Verfahrens muß zuverlässig ausgeschlossen sein. Die Verpflichtungserklärung muß in diesem Fall die Versendung der Bescheide mitumfassen.

Voraussetzung für die Beauftragung einer Firma ist in jedem Fall, daß das Steueramt seine Aufgaben nicht mit eigenen Kräften bewältigen kann.

11. Personalwesen

11.1 Personalaktenrecht

Durch das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften hat der Bundesgesetzgeber das Personalaktenrecht im **Bundesbeamtengesetz** und im **Beamtenrechtsrahmengesetz** neu geregelt. Die Änderungen sind am 1. Januar 1993 in Kraft getreten.

Zur Umsetzung des Rahmenrechts liegt dem Landtag der Entwurf eines Zwölften Gesetzes zur Änderung beamtenrechtlicher Vorschriften vor.

Der Gesetzentwurf enthält zahlreiche **positive Ansätze:** Der innerbehördliche Zugriff auf die Personalakte wird beschränkt, die Vorlage von Personalakten sowie die Auskunft hieraus werden auf das erforderliche Maß reduziert. Dem Beamten soll vor der Aufnahme von belastenden Unterlagen in die Personalakte ein Recht zur Äußerung zustehen. Weiterhin sind Regelungen zur Aufbewahrungsdauer von Personalakten und zur automatisierten Verarbeitung und Nutzung von Personalaktendaten vorgesehen.

Insbesondere die aus dem Rahmenrecht unverändert übernommenen Formulierungen zur **Verwendung von Personalakten und Beihilfeteilakten** sowie zur **Vorlage von Personalakten** und der **Auskunft** daraus werden dazu führen, daß die in manchen Bereichen bisher geübte Praxis künftig nicht mehr oder nur nach einer Verfahrensänderung zulässig sein wird. Dies betrifft die Veröffentlichung von Personalnachrichten im Staatsanzeiger, die Übertragung der Beihilfesachbearbeitung auf Dritte und die im Zusammenhang mit Ordensangelegenheiten eingeholten Auskünfte.

Ich habe das Staatsministerium der Finanzen um Stellungnahme gebeten.

11.2 Prüfung von DIAPERS

Im Berichtszeitraum habe ich bei zwei Regierungen und einer Universität die dort verwendete Version des Personal- und Stellenverwaltungssystems DIAPERS datenschutzrechtlich geprüft. Gegenstand der Kontrolle waren die Erhebung von Personaldaten von Betroffenen mit

Hilfe von **Formularen** – als Grundlage für die Datenspeicherung in DIAPERS –, die in DIAPERS-Person gespeicherten **Datengruppen,** die aus DIAPERS gefertigten **Auswertungen,** die neben DIAPERS geführten **Personalkarteien** sowie **Datenübermittlungen** aus DIAPERS und aus Personalkarteien.

Im einzelnen wurden folgende Feststellungen getroffen:

In meinem 14. Tätigkeitsbericht (Seite 69, Nr. 11.3) habe ich zur **Gestaltung eines Personalbogens** Stellung genommen. Ich habe darauf hingewiesen, daß für den Betroffenen die Rechtsvorschrift für die jeweilige Datenerhebung ersichtlich sein muß. Außerdem habe ich angeregt, die Frage nach der Religionszugehörigkeit künftig entfallen zu lassen. Eine Ausnahme ist im Geltungsbereich von Art. 1 Volksschulgesetz gegeben. Danach ist bei der Verwendung von Volksschullehrern auf die Bekenntniszugehörigkeit der Schüler Rücksicht zu nehmen. Diese Forderungen habe ich auch gegenüber den geprüften Stellen erhoben.

Der Entwurf eines 12. Gesetzes zur Änderung beamtenrechtlicher Vorschriften sieht auch die Änderung des Bayer. Beamtengesetzes vor. Nach Art. 100 Satz 2 EBayBG soll in Zukunft für Fragebögen, mit denen personenbezogene Daten u.a. im Zusammenhang mit der Begründung eines Dienstverhältnisses erhoben werden, die Genehmigung der obersten Dienstbehörde erforderlich sein. Ich habe die Staatsministerien des Innern und für Unterricht, Kultus, Wissenschaft und Kunst im Hinblick darauf gebeten, einen **datenschutzgerechten,** soweit möglich auch **einheitlichen Personalbogen für den Geschäftsbereich** zu entwickeln.

Datenspeicherung

Anhand der vorgelegten Datensatzbeschreibungen zu DIAPERS-Person wurden **Umfang** und **Erforderlichkeit** der Datenspeicherung sowohl in der Version für die Innere Verwaltung als auch in der Version für den Geschäftsbereich des Staatsministeriums für Unterricht, Kultus, Wissenschaft und Kunst überprüft. Zu beachten waren dabei auch die zwischen den Ministerien und dem jeweiligen Hauptpersonalrat abgeschlossenen **Dienstvereinbarungen.** Außerdem habe ich stichprobenartig Eintragungen in sogenannten **Freitextfeldern** überprüft.

Die Dienstvereinbarungen sehen vor, daß einige im Datensatz enthaltene Datenfelder nicht ausgefüllt werden dürfen. Außerdem wurden temporäre Löschungsregelungen vereinbart, d.h. Merkmale sind bei Eintritt bestimmter zeitlicher oder dienstrechtlicher Bedingungen zu löschen, wobei allerdings kein automatischer Löschlauf vorgesehen ist.

Auf meinen Wunsch hin durchgeführte **Sonderauswertungen** aus dem jeweiligen Datenbestand haben ergeben, daß in einzelnen Altfällen **entgegen den Dienstvereinbarungen** Daten noch nicht in der automatisierten Datei gelöscht worden waren. So wurden die **Prüfungsnote** und die **Platzziffer** der Anstellungsprüfung unbefristet vorgehalten, obwohl beide Daten nach drei Regelbeurteilungen bzw. der Lebenszeitverbeamtung gelöscht werden sollten. Ich habe die Löschung dieser Daten gefordert. Seit ca. 2 Jahren werden diese Daten programmgesteuert automatisch gelöscht, sobald ihre Speicherung nicht mehr zulässig ist, so daß künftig die Einhaltung der Dienstvereinbarung auf sachbearbeiterfreundliche Art sichergestellt ist.

In beschränktem Umfang können die Personalsachbearbeiter zu einzelnen Datengruppen auch frei formulierte Texte in sog. **Freitextfeldern** (Ergänzungsfeldern) in den Datenbestand eingeben. Ich habe stichprobenweise Datenblätter von Beschäftigten erstellen lassen, bei denen mindestens eines dieser Ergänzungsfelder besetzt war. Unzulässige Eintragungen wurden nicht festgestellt.

Auswertungen

Das Personal- und Stellenverwaltungssystem DIAPERS bietet auch die Möglichkeit, Auswertungen aus dem gespeicherten Datenbestand zu erstellen. Dies kann durch (festprogrammierte) **Standardlisten** oder durch in beschränktem Umfang frei gestaltbare **Varialisten** geschehen.

Aus dem Datenkatalog von DIAPERS sind zur Zeit **nur wenige Merkmale kombinierbar.** Nicht verknüpfbar sind insbesondere das Datum Beurteilung und die Freitextfelder. Hinweise darauf, daß entgegen den getroffenen Dienstvereinbarungen durch Auswertung Persönlichkeits- oder Leistungsprofile erstellt wurden, haben sich nicht ergeben.

Zugriffsberechtigungen

Bei der Vergabe der Zugriffsberechtigung ist neben der Abgrenzung, auf welche Datenmenge (Personalkategorie) der einzelne Bearbeiter zugreifen darf, auch darüber zu entscheiden, welche Funktionen (Arbeitsschritte) ausgeführt werden dürfen.

Die Festlegung der Zugriffsberechtigung ist der EDV-Abteilung schriftlich mitzuteilen. Dort erfolgt eine Speicherung in der DIAPERS-Schutzdatei und eine Protokollierung.

Bei einer der geprüften Stellen stimmten die in der Schutzdatei hinsichtlich der Personalkategorien gespeicherten Zugriffsberechtigungen teilweise nicht mit der tatsächlichen Sachbearbeitung in den einzelnen Referaten überein. Dieser Zustand bestand bereits seit rund zwei Jahren.

Ich habe gebeten, die vorgegebenen Zugriffsberechtigungen unverzüglich zu überprüfen.

Personalkarteien

Neben der Speicherung von Personaldaten in DIAPERS werden oftmals auch noch Personalkarteien geführt. Dies wird damit begründet, daß noch nicht alle Daten in DIAPERS übernommen sind.

In den Dienstanweisungen ist die Auflösung der Personalkarteien angeordnet, sobald diese entbehrlich sind.

In einer **Urlaubskartei** wurde bei Schwerbehinderten auf der Karteikarte auch der Grad der Erwerbsminderung vermerkt. Dieses Datum ist zur Aufgabenerfüllung nicht erforderlich. Es genügt die Angabe, daß aufgrund der **Schwerbehinderteneigenschaft** ein Anspruch auf Zusatzurlaub besteht.

11.3 Recht des behördlichen Datenschutzbeauftragten auf Einsichtnahme in Personalakten

Aufgrund einer Anfrage hatte ich mich zur Stellung des behördlichen Datenschutzbeauftragten zu äußern.

Die behördlichen Beauftragten für den Datenschutz sind in Bayern nicht gesetzlich verankert. Ihre Bestellung richtet sich vielmehr nach den Vollzugsbekanntmachungen zu Art. 26 Abs. 1 BayDSG. Zur Stellung des behördlichen Datenschutzbeauftragten und zum Grad seiner Weisungsfreiheit enthält die Bayerische Vollzugsbekanntmachung keine Vorgaben. Unmittelbare **Weisungsrechte** stehen ihm nur insoweit zu, als er nach interner Geschäftsverteilung im **Auftrag des Behördenleiters** dazu ausdrücklich befugt wird.

Hieraus folgt, daß der behördliche Beauftragte für den Datenschutz nicht eine aus der Verwaltung herausgelöste Stellung einnimmt, etwa wie der Landesbeauftragte für den Datenschutz, sondern als Mitarbeiter innerhalb der Behörde mit der Wahrnehmung einer bestimmten Aufgabe betraut ist. Nur in diesem Rahmen hat er auf die Beachtung der Datenschutzbestimmungen hinzuwirken. Verantwortlich für die Einhaltung des Datenschutzes bleibt die Behörde.

Die Befugnis des Behördenleiters, sich über den Verwaltungsvollzug im Rahmen der Dienstaufsicht – auch im Einzelfall – zu informieren, enthält auch sein Recht, in Personalakten Einsicht zu nehmen, die durch seine Behörde zu führen sind. Ein Einsichtsrecht des behördlichen Datenschutzbeauftragten ist nur gegeben, soweit dies **auf Weisung des Behördenleiters** geschieht. Ohne eine solche Weisung steht künftig einer Akteneinsicht auch Art. 100 a Abs. 3 Bayer. Beamtengesetz (BayBG) i.d.F. des Entwurfs eines Zwölften Gesetzes zur Änderung beamtenrechtlicher Vorschriften entgegen (deckungsgleich mit § 56 Abs. 3 Beamtenrechtsrahmengesetz (BRRG) bzw. § 90 Abs. 3 Bundesbeamtengesetz (BBG)). Danach dürfen Zugang zum Personalakt nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind.

11.4 Inhalt von Personalbögen

Im 14. Tätigkeitsbericht (Seite 69, Nr. 11.3) habe ich zum Inhalt des überarbeiteten Personalbogens für Beschäftigte eines Ministeriums Stellung genommen. Das Staatsministerium ist meinen Empfehlungen weitgehend nachgekommen. Strittig ist noch die Frage nach der **Religionszugehörigkeit** des Stellenbewerbers.

Das Staatsministerium führt aus, daß es aufgrund seiner Zuständigkeit für die Beziehung des Staates zu den Religionsgemeinschaften notwendig sei zu wissen, welche Mitarbeiter für entsprechende Tätigkeiten in Frage kommen.

Diese Argumentation konnte mich nicht überzeugen. Mit der Pflege der Beziehungen zu den Religionsgemeinschaften dürften in der Regel nur wenige Mitarbeiter beschäftigt sein. Es ist nicht einsehbar, daß auch für die bei weitem größere Zahl von Mitarbeitern die anderweitig beschäftigt sind, dieses Merkmal erhoben wird.

11.5 Übersendung von Personalakten an Verwaltungsgerichte bei sogenannten Konkurrentenklagen

Eine Stadt hat mich um Stellungnahme zu Datenübermittlungen bei sogenannten Konkurrentenklagen gebeten. Mit Klagen dieser Art wird von einem bei einer Personalentscheidung nicht zum Zuge gekommenen Beamten eine verwaltungsgerichtliche Nachprüfung der Maßnahme angestrebt. Das Verwaltungsgericht fordert in diesem Zusammenhang Unterlagen an. In dem von der Stadt geschilderten Fall verlangte das Verwaltungsgericht die Vorlage einer **Bewerberliste** und einer **Stellungnahme des Gesamtpersonalrats.**

Die Bewerberliste enthielt **Name**, Geburtsdatum, Familienstand, Kinderzahl, Ranglistennummer, Prüfungsjahrgang, Platzziffer und Prüfungsnote der Anstellungsprüfung sowie die Gesamtergebnisse der letzten beiden periodischen Beurteilungen, das Datum des Diensteintritts und den Zeitverlauf des beruflichen Werdegangs. Die Angaben erfolgten für 13 gehobene Beamte der Stadt, die sich auf die Stellenausschreibung hin beworben hatten. Sie stellten eine **Kurzfassung der jeweiligen Personalakte** dar. Die Stellungnahme des Gesamtpersonalrats enthielt dessen Zustimmung zum Auswahlverfahren und zur getroffenen Entscheidung.

Nach meiner Ansicht ist die Prüfung zweier unterschiedlicher Datenübermittlungen veranlaßt. Zum einen liegt eine Übermittlung der Personalabteilung der beklagten Behörde an das **Verwaltungsgericht** vor, zum anderen ist die Übermittlung aus den Gerichtsakten an den **Rechtsanwalt des Klägers** bzw. an den Kläger selbst datenschutzrechtlich zu bewerten.

Übermittlung an das Gericht

Die Aktenanforderungspraxis Bayer. Verwaltungsgerichte im Rahmen von Konkurrentenklagen ist unterschiedlich. Sie stützt sich auf § 99 Verwaltungsgerichtsordnung (VwGO). Danach sind Behörden zur Vorlage von Urkunden, Akten und zu Auskünften verpflichtet. Allerdings kann die zuständige oberste Aufsichtsbehörde die Vorlage oder Auskunft verweigern, wenn die Vorgänge u.a. nach einem Gesetz oder ihrem Wesen nach geheimgehalten werden müssen. § 99 VwGO geht als lex specialis den Datenschutzgesetzen des Bundes und der Länder vor.

Enthalten vorhandene Verwaltungsvorgänge drittbezogene Angaben schutzwürdiger Art, für die nicht ausgeschlossen werden kann, daß sie für die Entscheidung des anhängigen Rechtsstreits auch nur möglicherweise von Bedeutung sein können, so hat die Behörde unter Berücksichtigung der in der Rechtsprechung hierzu entwickelten Grundsätze (vgl. insbesondere die „Scheidungsaktenbeschlüsse" BVerfGE 27, 344 und BVerfGE 34, 205 sowie die zur Frage der Beiziehung von Personalakten Unbeteiligter ergangene Entscheidung BVerwGE 19, 179) **Belange dieser Dritten** mit dem Anspruch des Klägers auf **effektiven Rechtsschutz** und dem öffentlichen Interesse an einem **ungehinderten Gang der Rechtspflege abzuwägen.** Gelangt sie dabei zu dem Ergebnis, daß die datenschutzrechtlichen Belange überwiegen und deshalb Vorgänge geheimzuhalten sind, so hat sie gemäß § 99 Abs. 1 Satz 2 VwGO die Entscheidung ihrer obersten Aufsichtsbehörde einzuholen. Teilt diese den Standpunkt der aktenführenden Stelle, daß der fragliche Vorgang „seinem Wesen nach" geheimzuhalten sei, so kann der Kläger die **„Sperrerklärung"** der obersten Aufsichtsbehörde im **Zwischenverfahren** nach § 99 Abs. 2 VwGO nachprüfen lassen. Letztlich befinden damit die Gerichte über den Umfang der ihnen vorzulegenden Unterlagen.

Die angesprochene Bewerberliste umfaßt dem Personalaktengeheimnis unterliegende Angaben des bei der Stellenausschreibung zum Zuge gekommenen Beamten, des Klägers und weiterer ebenfalls unterlegener 11 Beamten.

Sie enthält keine im Blick auf die zu treffende Entscheidung wesensfremden Merkmale. Die Angaben sind für die Entscheidung des Verwaltungsgerichts erforderlich. Das Gericht sollte allerdings das Bewerberverzeichnis nur in **teilanonymisierter Form** anfordern bzw. erhalten.

Die Teilanonymisierung könnte dadurch erreicht werden, daß hinsichtlich der anderen (11) Mitbewerber auf die Angabe des Namens verzichtet und das Geburtsdatum durch das Lebensjahr ersetzt wird. Auf – evtl. auch späteren – Wunsch des Gerichts wären die Namen allerdings bekanntzugeben.

Auch die Stellungnahme des Gesamtpersonalrats kann – teilanonymisiert – vorgelegt werden, da sie nach Schilderung der Stadt keine drittbezogenen Angaben enthält.

Auf erhebliche Bedenken würde stoßen, wenn das Verwaltungsgericht die gesamten Personalakten des erfolgreichen Bewerbers und der unterlegenen Mitbewerber anfordern würde. Personalakten enthalten in einer Vielzahl von Fällen persönliche Angaben, die keinen sachlichen Zusammenhang mit dem vor Gericht anhängigen Rechtsstreit aufweisen.

In der Praxis wird gleichwohl oftmals die Akte komplett zur Verfügung gestellt. Begründet wird dies mit der Erfahrung, daß die Kläger auf eine selektive Aktenvorlage, auch wenn sie sachlich gerechtfertigt ist, nicht selten mit gesteigertem Mißtrauen gegen die Verwaltung und deren Prozeßführung reagieren. Diese Praxis entspricht nicht dem § 99 VwGO. Nach dieser Bestimmung sind nur solche Unterlagen vorzulegen, „deren Inhalt der umfassenden Sachverhaltsaufklärung durch das Gericht und der Gewinnung von Grundlagen für die Führung des anhängigen Prozesses überhaupt dienlich sein kann" (BVerwGE 15, 132). Auf Unterlagen, die keinen auch noch so entfernten Bezug zur anhängigen Streitsache aufweisen, erstreckt sich die Vorlagepflicht der Verwaltung nach § 99 Abs. 1 Satz 1 VwGO von vornherein nicht.

Will die Verwaltung von der Möglichkeit Gebrauch machen, sachlich nicht einschlägige, aber formell zum „Vorgang" gehörige Unterlagen aus datenschutzrechtlichen Gründen von der Übersendung an das Gericht auszunehmen, so bietet sich an, daß sie die hierfür maßgeblichen Gründe offenlegt und dabei den Inhalt der einbehaltenen Aktenbestandteile in einer Weise beschreibt, die dem Gericht und den übrigen Beteiligten eine Beurteilung der tatsächlichen Entscheidungserheblichkeit ermöglicht. Unter dieser Voraussetzung ist gewährleistet, daß letztverantwortlich das Gericht und nicht die beklagte Behörde darüber befindet, ob Aktenbestandteile möglicherweise entscheidungserheblich und deshalb vorzulegen sind.

Teilt in einem solchen, nicht nach § 99 Abs. 1 Satz 2 VwGO abgewickelten Fall, zwar das Gericht, nicht aber der Kläger die Auffassung der Behörde von der Unbehelflichkeit der nicht übersandten Aktenteile, so hat letzterer die Möglichkeit, durch einen entsprechenden Beweis- oder Beweisermittlungsantrag ihre Beiziehung förmlich zu beantragen. Dringt er damit nicht durch, so kann er gegen die instanzbeendende Entscheidung, sofern sie anfechtbar ist, Rechtsmittel einlegen und hierbei geltend machen, das Gericht sei seiner Verpflichtung zur Sachverhaltsaufklärung (§ 86 Abs. 1 VwGO) nicht nachgekommen.

Verlangt hingegen das Gericht von sich aus oder auf entsprechende Forderung des Klägers hin die Vorlage der einbehaltenen Aktenstücke und hat die aktenführende Stelle weiterhin Bedenken, dem gerichtlichen Ersuchen zu entsprechen, so bestimmt sich das weitere Verfahren nach § 99 Abs. 1 Satz 2, Abs. 2 VwGO.

Datenübermittlung aus den Gerichtsakten an den Rechtsanwalt des Klägers bzw. an den Kläger

Nach § 100 VwGO können die Beteiligten die dem Gericht vorgelegten Unterlagen **einsehen.** Dabei kann nicht ausgeschlossen werden, daß solche Unterlagen personenbezogene Daten enthalten, deren Offenbarung nicht zwingend erforderlich oder aus datenschutzrechtlicher Sicht nicht vertretbar ist.

In diesem Zusammenhang ist Art. 19 Abs. 4 GG zu beachten. Danach steht jedem Bürger der Rechtsweg offen, wenn er durch die öffentliche Gewalt in seinen Rechten verletzt wird. Bei einer Konkurrentenklage wäre ein lückenloser und effektiver Rechtsschutz nicht mehr gegeben, wenn eine im Grunde zulässige Klage nicht begründet werden könnte, weil personenbezogene Daten

von Konkurrenten nicht in den Prozeß eingebracht werden können.

Die vorstehend ausführlich beschriebene gegenwärtige Rechtslage vermag nicht in allen Fällen zu befriedigen.

Zum einen erscheint die Annahme nicht lebensfremd, daß der Kläger bei Konkurrentenklagen die durch Akteneinsicht bei Gericht gewonnenen – vermeintlich negativen – Erkenntnisse über seinen Konkurrenten auch außerhalb des eigentlichen Gerichtsverfahrens (etwa bei Kollegen, am Stammtisch u.ä.) verbreitet und entsprechend kommentiert. Zum anderen könnte die Konkurrentenklage auch bei aussichtslosen Fällen als Instrument dienen, sich (legal!) persönlichkeitsrechtsrelevante Informationen über konkurrierende Kollegen zu beschaffen. Erwägenswert erscheint mir eine gesetzliche strafbewehrte Bestimmung, wonach das Gericht den Prozeßparteien die außergerichtliche Nutzung von Daten, die sie im Prozeß erfahren haben, verbieten kann (vgl. auch Nr. 6.8.3).

Ich werde mich mit diesem Anliegen nochmals an die Staatsregierung wenden.

11.6 Schutz von Personaldaten im Hochschulbereich

Aufgrund einer Anfrage hatte ich mich mit der Verwendung von Personaldaten einer Universität in einem elektronisch abrufbaren Mail-Box-System und in einem herkömmlichen Personen- und Einrichtungsverzeichnis zu befassen.

1. Mail-Box-System

   Eine Universität will aus ihrem Personaldatenbestand Daten über Wissenschaftler in ein international verfügbares Mail-Directory-System übernehmen. Damit soll die weltweite Kommunikation zwischen den Wissenschaftlern gefördert werden. Es soll ein Verzeichnis erstellt werden, das die Gliederung der Universität bis zur Lehrstuhlebene wiedergibt und innerhalb der Lehrstühle die wissenschaftlichen Mitarbeiter enthält. Über die betroffenen Personen sollen folgende Daten in das Verzeichnis aufgenommen werden: Name, Vorname, Titel, Stellung (z.B. wissenschaftlicher Mitarbeiter) und Institutszugehörigkeit, dienstliche Postadresse, dienstliche Telefonnummer, dienstliche Fax-Nummer und E-Mail-Adresse. Diese Daten sind über den Directory-Verbund weltweit uneingeschränkt lesbar. Mit Ausnahme der E-Mail-Adresse sind die vorgenannten Daten bereits dem öffentlich erhältlichen Personen- und Einrichtungsverzeichnis der Universität zu entnehmen. Jeder Betroffene soll persönlich die Möglichkeit erhalten zu entscheiden, ob seine Daten nur in der Universität oder weltweit verfügbar sein sollen. Desweiteren soll jeder seine Daten auch modifizieren oder auch ganz streichen lassen können.

   Unter diesen Voraussetzungen halte ich die Beteiligung der Universität am Mail-Directory-System aus datenschutzrechtlicher Sicht, unter Heranziehung der Rechtsgedanken aus Art. 18 Abs. 1 Bayer. Datenschutzgesetz (BayDSG) bzw. Art. 19 Abs. 1 BayDSG neu für zulässig. Die Beteiligung am Mail-Box-System ist zur Aufgabenerfüllung der Universität erforderlich, da es die direkte Kontaktaufnahme zwischen Wissenschaftlern weltweit ermöglicht und damit Forschungsarbeiten erleichtert. Die Daten können bereits dem veröffentlichten Personen- und Einrichtungsverzeichnis entnommen werden. Durch das vorgesehene Dispositions- bzw. Widerspruchsrecht wird eine Beeinträchtigung persönlicher Belange ausgeschlossen.

   Dabei bin ich davon ausgegangen, daß alle Betroffenen rechtzeitig vor Aufnahme in das Verzeichnis durch eine persönliche Mitteilung zuverlässig darüber unterrichtet werden, welche Daten das Verzeichnis enthalten soll und, daß ein Dispositions- bzw. Widerrufsrecht gegen die Aufnahme in das Mail-Box-Verzeichnis besteht.

   Diese Widerspruchsregelung anstatt der Einwilligung jedes Betroffenen halte ich in vorliegendem Fall für ausreichend, weil ausschließlich solche Personen in das E-Mail-System einbezogen werden, deren Daten bereits (seit Jahren) im Personenverzeichnis der Universität veröffentlicht werden.

   Gegen die Gestaltung des Abrufverfahrens dergestalt, daß der Zugriff, in entsprechend eingeschränkter Form, unmittelbar auf das **universitätseigene Personalverwaltungssystem** anstelle einer **physisch eigenen Datei** für das E-Mail-Verfahren erfolgt, habe ich aus Gründen der gebotenen Datensicherung massive Bedenken erhoben. An die Ausgestaltung der Datensicherungsmaßnahmen müssen hohe Anforderungen gestellt werden.

2. Personen- und Einrichtungsverzeichnis

   Bei Durchsicht des Personen- und Einrichtungsverzeichnisses einer Universität habe ich festgestellt, daß die **Privatadressen** des Lehrpersonals und bei einzelnen wissenschaftlichen Einrichtungen zum Teil auch **Hilfspersonal** wie Krankenschwestern und Mechaniker **namentlich** aufgeführt wurden. Es ist nicht erkennbar, daß die Veröffentlichung solcher Daten zur Erfüllung von Aufgaben der Universität erforderlich sein soll. Auch ein berechtigtes Interesse Dritter, die das Verzeichnis kaufen, ist nicht ersichtlich. Vielmehr kann für die Betroffenen ein erhebliches schutzwürdiges Interesse am Ausschluß einer solchen Übermittlung bestehen. Nach dem Datenschutzrecht ist die Bekanntgabe dieser Daten an Dritte unzulässig (Art. 18 Abs. 1 BayDSG, künftig Art. 19 Abs. 1 BayDSG neu). Die Veröffentlichung ist nur mit **Einwilligung** der Betroffenen möglich. Die Einwilligung ist im Regelfall bei neuen Mitarbeitern der Universität in **Schriftform** einzuholen. Bei Mitarbeitern, die im letzten Personenverzeichnis

bereits veröffentlicht wurden, kann dagegen von einer mutmaßlichen Einwilligung ausgegangen werden, wenn sie in geeigneter Form über eine Widerspruchsmöglichkeit gegen die erneute Aufnahme der Privatadresse in das Personenverzeichnis informiert wurden.

11.7 Herausgabe von Lohnkonten und Dienststundennachweisen an einen Zweckverband

In einem Zweckverband Abfallwirtschaft stellen die Gemeinden Personal für Recyclinghöfe des Zweckverbandes. Die Personalkosten erhalten sie vom Zweckverband gegen Vorlage detaillierter Nachweise ersetzt. Der Zweckverband hat deshalb Lohnkonten, Dienststundennachweise usw. angefordert. Der Zweckverband hat angefragt, ob datenschutzrechtliche Gründe einer Übermittlung von Personaldaten der Mitgliedsgemeinden an den Zweckverband entgegenstehen.

Soweit die Übermittlung von **anonymisierten Unterlagen** zur Aufgabenerfüllung ausreicht, ist die Übermittlung von personenbezogenen Personaldaten nicht erforderlich und daher unzulässig. Da bei dieser Datenübermittlung abgebende und empfangende Stelle öffentliche Stellen sind, besteht im Normalfall ein ausreichendes Vertrauensverhältnis, so daß der Zweckverband eine vom Bürgermeister der Gemeinde unterschriebene Erklärung über die entstandenen Lohnkosten/Dienststunden als ausreichenden Nachweis akzeptieren kann. Ein solcher Nachweis kann auch ohne Angabe der Namen von Gemeindebediensteten die Lohnkosten und Dienststunden detailliert ausweisen. Erst wenn Zweifel an der Richtigkeit einer anonymisierten Aufstellung auftreten, stellt sich die Frage nach Belegen mit den Namen der eingesetzten Personen.

Da der Zweckverband anschaulich darlegen konnte, daß in der augenblicklichen Anlaufphase in einer Vielzahl von Fällen Fehlabrechnungen bei den Gemeinden festzustellen waren und dies aufgrund der großen Anzahl der vom Zweckverband unterhaltenen Recyclinghöfe erhebliche finanzielle Auswirkungen hat, werde ich zur Vermeidung dieser Fehlberechnungen das augenblickliche personenbezogene Abrechnungsverfahren während einer begrenzten Übergangszeit nicht beanstanden.

11.8 Übermittlung von Personaldaten an Krankenversicherungen für Werbezwecke

Die Personalverwaltung einer Gemeinde hat mich um Stellungnahme gebeten, ob sie Anfragen von privaten Krankenkassen beantworten darf, in denen die Namen aller Gemeindebediensteten angefordert werden.

Ich habe dazu folgende Auffassung vertreten:

Bei einer Datenübermittlung an private Krankenkassen handelt es sich um eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches, so daß sich die Übermittlung nach Art. 18 Abs. 1 Bayer. Datenschutzgesetz (BayDSG) richtet. Nach Art. 18 Abs. 1 BayDSG ist eine Übermittlung personenbezogener Daten u.a. zulässig, soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Zwar kann ein berechtigtes Interesse der Versicherungsunternehmen an der Kenntnis von Namen der bei der Gemeindeverwaltung Beschäftigten nicht ausgeschlossen werden. Berechtigtes Interesse ist nämlich jedes von der Rechtsnorm anerkannte Interesse. Dazu zählt auch ein wirtschaftliches Interesse, wozu das Versenden von Werbematerial bzw. die Anbahnung von Vertragsverhandlungen gehört.

Einer Datenübermittlung stehen jedoch schutzwürdige Belange der betroffenen Personen entgegen, insbesondere deren Recht auf Wahrung der Privatsphäre, das aus dem allgemeinen Persönlichkeitsrecht abgeleitet ist. Der Einzelne hat ein Recht darauf, daß seine Privatsphäre nicht durch die unerwünschte Zusendung von Werbematerial beeinträchtigt wird. Dabei ist zu berücksichtigen, daß die Zusendung von Werbematerial zunehmend als Belästigung empfunden wird.

Datenübermittlungen der geschilderten Art sind deshalb nur mit Zustimmung des betroffenen Mitarbeiters zulässig (Art. 4 Abs. 1 Nr. 2 BayDSG).

Zum gleichen Ergebnis führt Nr. 18.2.4 der Vollzugsbekanntmachung zum BayDSG. Danach sollen Auskünfte über mehrere vom Empfänger nicht namentlich bezeichnete Personen (Gruppenauskünfte) im Regelfall nur erteilt werden, wenn sie im öffentlichen Interesse liegen. Fehlt ein öffentliches Interesse (z.B. bei listenmäßigen Übermittlungen von Daten zu Werbezwecken), darf Auskunft nur erteilt werden, wenn die Betroffenen zugestimmt haben.

11.9 Übermittlung von Personaldaten im Zusammenhang mit der Bestellung von Schöffen

Eine Bürgerin hat sich an mich gewandt mit der Bitte zu prüfen, ob ihr Dienstherr berechtigt war, im Rahmen ihrer Bestellung zur Schöffin dem Landgericht Angaben über ihre Krankheitstage, noch nicht beanspruchten Urlaubstage sowie ihre bevorstehende Versetzung in den Ruhestand weiterzuleiten. Der Dienstherr hatte mit diesen Angaben einen Antrag begründet, die Petentin wegen des großen Arbeitsanfalls vom Schöffendienst zu entbinden.

Ich habe die Weitergabe der Angaben als für nicht zulässig angesehen.

Angaben über Krankheitstage, noch ausstehenden Resturlaub und die bevorstehende Versetzung in den Ruhestand sind wohl der Personalakte und ggf. geführten Karteien zu Urlaubs- und Krankheitstagen entnommen worden. Wegen derzeit noch fehlender besonderer Vorschriften zum Personalaktenrecht ist die Weitergabe der o. g. Daten an das Landgericht an Art. 17 BayDSG zu messen,

weil es sich hier um die Übermittlung personenbezogener Daten an andere öffentliche Stellen handelt. Diese ist nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgaben erforderlich ist.

Die Datenübermittlung war nicht zur Aufgabenerfüllung des Empfängers, des Landgerichts, nötig. Sie fiel auch nicht in den Aufgabenbereich des Dienstherrn, denn nach § 54 Abs. 1 i.V.m. § 77 Abs. 1 Gerichtsverfassungsgesetz kann der zuständige Richter beim Landgericht einen Schöffen nur **auf dessen Antrag** von der Dienstleistung an bestimmten Sitzungstagen entbinden, wenn Hinderungsgründe eintreten.

Der Antrag, vom Schöffendienst entbunden zu werden, kann also **nur vom Schöffen selbst** und nicht z. B. von dessen Arbeitgeber gestellt werden. Für diesen wäre es nur möglich gewesen, seine zum Schöffendienst bestellte Arbeitnehmerin zu bitten, einen entsprechenden Antrag zu stellen.

11.10 Regelmäßige Herausgabe von Lohnkonten an das Kreisrevisionsamt

Ein Kreisrevisionsamt hat vom Hauptamt eines Landkreises die regelmäßige Übergabe der Lohnkonten des jeweils abgelaufenen Kalendermonats sämtlicher Bediensteter gefordert. Das Hauptamt des Landkreises hat die Rechtmäßigkeit dieser Anforderung bezweifelt und mich um Stellungnahme gebeten.

Im Einvernehmen mit den Staatsministerien des Innern und der Finanzen habe ich folgende Auffassung vertreten: Eine regelmäßige Weitergabe sämtlicher monatlicher Lohnkonten an das Rechnungsprüfungsamt ist für eine ordnungsgemäße und ausreichende Rechnungsprüfung nicht erforderlich.

Davon nicht berührt ist das Recht des Rechnungsprüfungsamtes, stichprobenartige Prüfungen sämtlicher Lohnkonten eines oder mehrerer Monate vorzunehmen. Auch im Bereich der sogenannten **mitschreitenden Prüfung** der Bezügeabrechnungen durch die Rechnungsprüfungsämter im staatlichen Bereich erfolgt keine regelmäßige Weitergabe aller Lohnkonten.

Im Ergebnis ist der dargestellte Sachverhalt wie die von mir bereits einmal aufgegriffene regelmäßige Weiterleitung von Beihilfedaten an ein Rechnungsprüfungsamt zu beurteilen. Auch diese habe ich für nicht zulässig gehalten. Meine Stellungnahme ist dem 14. Tätigkeitsbericht (Seite 62, Nr. 7.12) zu entnehmen.

11.11 Auswertung von Daten aus einer Arbeitsbelastungsuntersuchung bei Forstämtern für die Beurteilung des Personals

Das Staatsministerium für Ernährung, Landwirtschaft und Forsten hatte für bestimmte Forstämter eine Arbeitsplatzuntersuchung angeordnet. Im Schreiben an die Oberforstdirektion wurde als Grund „eine objektivierbare Einschätzung der Arbeitsbelastung" angegeben. Die Oberforstdirektion begründete die Erhebung gegenüber den Forstämtern mit einer „objektiveren Einschätzung der Arbeitsbelastung in den Forstämtern". Eine evtl. Verwendung der Daten für Beurteilungszwecke war in keinem der Schreiben erwähnt.

Von Betroffenen wurde nun die Frage aufgeworfen, ob die Daten auch für Beurteilungen herangezogen werden könnten. Es sei zwar nicht Ziel der Untersuchung, für bestimmte Personen Leistungsdaten zu erheben. Es sollte jedoch Klarheit darüber geschaffen werden, ob die zuständigen Vorgesetzten, welche die Daten aus der Untersuchung sehen, diese auch im Rahmen von Beurteilungen berücksichtigen dürften.

Das Ministerium und der Hauptpersonalrat hielten eine Verwendung der aus der Untersuchung gewonnenen Daten bei der Beurteilung zunächst für denkbar. Die datenschutzrechtliche Überprüfung ergab jedoch, daß eine solche Nutzung nicht zulässig wäre:

Aus Sicht des Datenschutzes ist von Bedeutung, daß die Daten für **Planungszwecke** und nicht für **Personalverwaltungszwecke** erhoben wurden. Damit handelt es sich nicht um Personaldaten. Auch als „Personalaktendaten" im Sinne des § 56 des geänderten Beamtenrechtsrahmengesetzes sind die Daten nicht anzusehen. Die Zulässigkeit einer Nutzung für andere als Planungszwecke, insbesondere für Beurteilungen, richtet sich daher nach allgemeinem Datenschutzrecht. § 56 Abs. 1 Satz 3 des Beamtenrechtsrahmengesetzes, wonach Personalaktendaten für Zwecke der Personalverwaltung und Personalwirtschaft grundsätzlich verwendet werden dürfen, bietet somit keine Interpretationshilfe.

Bei der Erhebung wurden die Bediensteten davon unterrichtet, daß die Betriebsdaten zur objektiven Einschätzung der Arbeitsbelastung dienen. Damit wurde der Erhebungszweck festgelegt. Die Betroffenen sind aus ihrer beamtenrechtlichen Treuepflicht heraus verpflichtet, dem Dienstherrn für Planungszwecke solche Angaben zu machen. Hiervon ist auszugehen, obwohl ein Hinweis auf die Pflicht zur Angabe bzw. zur Freiwilligkeit trotz Art. 16 Abs. 2 BayDSG nicht gegeben worden war. Das Fehlen eines solchen Hinweises ist ein weiteres Indiz dafür, daß es nicht Ziel der Erhebung war, **Leistungsdaten** über bestimmte oder bestimmbare Personen zu erheben. Hinzu kommt, daß es wohl die Gewinnung objektiver Angaben zur Arbeitsbelastung erschwert hätte, wenn die Untersuchung gleichzeitig zur Gewinnung von Beurteilungsgrundlagen für Beamte bestimmt gewesen wäre und dementsprechend gemäß Art. 16 Abs. 2 BayDSG auf dieses weitere Erhebungsziel gegenüber den Betroffenen hingewiesen worden wäre.

Die Erhebung von Planungsdaten über die Arbeitsbelastung bei den Forstämtern ähnelt vielmehr der Erhebung von Daten für amtliche Statistiken. Dort ist ausgeschlossen, die erhobenen Daten für andere Zwecke zu verwenden, damit die Angaben nicht mit Rücksicht auf andere Verwendungszwecke „geschönt" werden.

Eine Verwendung der erhobenen Arbeitsbelastungsdaten bei der dienstlichen Beurteilung wäre eine wesentliche Änderung des Verwendungszwecks und damit ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen. Eine gesetzliche oder sonstige Erlaubnis für einen solchen Eingriff fehlt.

Auch das künftige Bayerische Datenschutzgesetz gestattet eine solche Zweckänderung nicht. Eine Nutzungsänderung wäre danach allenfalls zulässig, wenn offensichtlich wäre, daß es im Interesse des Betroffenen liegt und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung hierzu verweigern würde. Das heißt: Eine Verwendung für Beurteilungszwecke wäre nach dem Datenschutzgesetz künftig nur zulässig, wenn sie zu einer besseren Beurteilung führen würde.

Auf meine Bitte hat das Ministerium zugesichert, daß die Planungsdaten nicht für Beurteilungszwecke genutzt werden.

12. Gewerbe und Handwerk

12.1 Prüfung eines Gewerbeamtes

Bei einer kreisangehörigen Gemeinde habe ich das Gewerbeamt und dort insbesondere die **Gewerbedatei** geprüft. Eine Gewerbekartei/-datei kann von der Gemeinde über alle ortsansässigen Gewerbetreibenden geführt werden. Diese müssen Beginn, Veränderung oder Aufgabe des Gewerbes nach den Bestimmungen der Gewerbeordnung (GewO) bei der Gemeinde anzeigen.

Die Gemeinde führt die Gewerbedatei in automatisierter Form, d.h., sie gibt die Daten, die sie von den Gewerbetreibenden über die Anzeigen nach den Bestimmungen der Gewerbeordnung erhält, in eine EDV-Anlage ein. Zwar entsprach die Datenerhebung, -speicherung und -übermittlung der Gewerbeordnung, der Gewerbeanzeigenverordnung und der Gewerbeanzeigenverwaltungsvorschrift. Die Gemeinde hat jedoch bisher bei abgemeldeten Gewerben weder die Datensätze der automatisierten Gewerbedatei noch die schriftlichen Unterlagen hierzu daraufhin überprüft, ob die Datensätze und Unterlagen noch zur Aufgabenerfüllung benötigt werden. Ich habe die Gemeinde deshalb aufgefordert, gemäß der allgemeinen Aussonderungsbekanntmachung (AllMBl Nr. 28/1991, Seite 884 ff.) eine **Aussonderung** durchzuführen.

12.2 Weitergabe von Daten aus der Gewerbekartei an einen Abwasserzweckverband

Eine Gemeinde fragte mich, ob es zulässig sei, Daten aus der Gewerbekartei an den Abwasserzweckverband, in dessen Einzugsgebiet die Gemeinde liegt, zu übermitteln.

Die Übermittlung personenbezogener Daten von einer Gemeinde an einen Abwasserzweckverband ist nach Art. 17 Abs. 1 BayDSG zulässig, wenn sie zur rechtmäßigen Erfüllung von Aufgaben erforderlich ist, die der übermittelnden Stelle oder dem Empfänger durch Rechtsnorm zugewiesen sind. Zu beachten ist außerdem die Allgemeine Verwaltungsvorschrift für die Behandlung von Anzeigen nach den §§ 14 und 55 c Gewerbeordnung (GewAnzVwv; Bekanntmachung des Bayerischen Staatsministeriums für Wirtschaft und Verkehr vom 2.11.1980, WVMBl 1/1980, S. 1 ff.). Die Gemeinde muß danach überprüfen, erforderlichenfalls aufgrund der entsprechenden Angaben durch den Abwasserzweckverband, ob für letzteren die angeforderten Daten ihrer Art nach zur Erfüllung einer durch Rechtsnorm zugewiesenen Aufgabe erforderlich sind (z.B. um die Art und Menge des Abwasseraufkommens oder den Verschmutzungsgrad festzustellen). Hierzu dürften wohl in der Regel die Angaben zum Namen des Gewerbetreibenden, zur betrieblichen Anschrift und zur angemeldeten Tätigkeit ausreichend sein.

12.3 Auskunft über Namen und Anschrift aller Gewerbetreibenden aus der Gewerbekartei an den örtlichen Gewerbeverein

Eine Gemeinde wollte wissen, ob es zulässig ist, die Namen und Anschriften aller Gewerbetreibenden an den örtlichen Gewerbeverein zu übermitteln. Dieser beabsichtigte, bei den Betroffenen für die Teilnahme an einem Bürgerfest zu werben. Ich habe der Gemeinde folgende datenschutzrechtliche Bewertung mitgeteilt:

Für die Gewerbetreibenden, die auf ihrer Gewerbeanzeige einer Datenübermittlung zu Werbezwecken nicht ausdrücklich zugestimmt haben, beurteilt sich die Weitergabe nach Art. 18 Abs. 1 BayDSG. Danach ist die Übermittlung an Dritte außerhalb des öffentlichen Bereichs zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht, und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden (Art. 18 Abs. 1 Satz 1 zweite Alternative). Bei Datenübermittlungen aus der Gewerbekartei ist außerdem die allgemeine Verwaltungsvorschrift für die Behandlung von Anzeigen nach den §§ 14 und 55 c Gewerbeordnung (GewAnzVwv; Bekanntmachung des Bayerischen Staatsministeriums für Wirtschaft und Verkehr vom 2. November 1980, WVBl 1/1980, S. 1 ff.) zu beachten. Diese enthält in Nr. 6.2. Hinweise zur Erteilung von Auskünften über Gewerbeanzeigen an Stellen außerhalb des öffentlichen Bereichs.

Bei der gewünschten Auskunft handelt es sich um eine Gruppenauskunft im Sinne von Nr. 6.2.2 GewAnzVwv, da sie sich auf eine Vielzahl nicht namentlich bezeichneter Gewerbetreibender zum Zwecke der Werbung bezieht. Da der Gewerbeverband kein Berufsverband im Sinne von Nr. 6.2.1 Abs. 1 Satz 2 letzter Halbsatz GewAnzVwv ist, kann die Auskunft nur über die Gewerbetreibenden erteilt werden, die einer derartigen Datenübermittlung (z.B. bei der Gewerbeanmeldung) **ausdrücklich zugestimmt** haben (vgl. Nr. 6.2.2 GewAnz-

Vwv). Die Gemeinde hätte sich allerdings bereit erklären können, für den Gewerbeverband die Einladungsschreiben an die örtlichen Gewerbebetriebe zu versenden.

12.4 Datenübermittlung aus der Lehrlingsrolle an berufsständische Versorgungseinrichtungen

Eine Handwerkskammer wollte wissen, ob sie Adressen aus der Lehrlingsrolle an die berufsständischen Versorgungseinrichtungen, die privatrechtlich organisiert sind, weitergeben kann.

Die Weitergabe beurteilt sich nach Art. 18 Abs. 1 BayDSG. Die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ist danach zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden (Art. 18 Abs. 1 Satz 1 zweite Alternative).

Mangels gesetzlicher Mitteilungspflichten bzw. -befugnisse dürfen die Adressen des betroffenen Personenkreises nur übermittelt werden, wenn die Betroffenen dazu eingewilligt haben, da ansonsten schutzwürdige Belange im Sinne der obengenannten Vorschrift beeinträchtigt würden. Die Betroffenen haben ein Recht darauf, daß ihre Privatsphäre nicht durch unerwünschte Zusendung von Werbematerialien beeinträchtigt wird.

13. Landwirtschaft

13.1 Integriertes Verwaltungs- und Kontrollsystem InVeKoS der EU-Mitgliedsstaaten im Bereich der Landwirtschaftsförderung

Die EU hat die Mitgliedsstaaten zur Einführung eines „Integrierten Verwaltungs- und Kontrollsystems (InVeKoS)" verpflichtet. Damit soll ein ordnungsgemäßer und einheitlicher Vollzug der EU-Agrarreform gewährleistet und insbesondere die mißbräuchliche Verwendung von Fördermitteln verhindert werden (Verordnung (EWG) Nr. 3508/92 des Rates vom 27. November 1992 und Verordnung (EWG) Nr. 3887/92 der Kommission vom 23. Dezember 1992). Hierzu werden von den Landwirtschaftsverwaltungen integrierte Datenbanken mit Angaben über Flurstücke, deren Nutzung sowie den Tierbestand eingerichtet und in einem Mindestumfang Kontrollen durchgeführt. Auch Fernerkundung durch Satellit oder Flugzeuge ist als Kontrollmittel vorgesehen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder in ihrer Konferenz am 26./27. Oktober 1993 hat die EU mit dem „Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot widersprechen kann. Insbesondere legt die Verordnung für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte haben die Datenschutzbeauftragten des Bundes und der Länder daher vor allem gefordert

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten **Stichprobenumfang** zu beschränken;
- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der **Verhältnismäßigkeit** und insbesondere der **Zweckbindung** zu beachten;
- nur **dezentrale Datenbanken** in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbanken über Landwirte!) und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln.

13.2 Datenschutz bei Kontrollstellen nach der EG-Verordnung über den ökologischen Landbau

Im Berichtszeitraum besuchte ich „Öko-Kontrollstellen", die nach der EG-Verordnung 2092/91 über den „ökologischen Landbau" eingerichtet wurden.

Die EG-Verordnung hat die Regierungen der Mitgliedsstaaten verpflichtet, ein Kontrollsystem für die Unternehmen einzurichten, die Produkte aus ökologischem Landbau herstellen und sie entsprechend kennzeichnen. Die Bundesländer konnten dabei wählen zwischen einer Organisationsform, bei der die Unternehmen durch staatliche Stellen direkt kontrolliert werden, und einer Form, bei der die Kontrolle von privaten Kontrollstellen nach einer Zulassung durch staatliche Behörden vorgenommen wird. Bayern hat sich, wie die anderen Bundesländer, für die Kontrolle durch private Kontrollstellen entschieden.

Die bayerischen Kontrollstellen führen das Kontrollverfahren als **beliehene Unternehmen** nach einer besonderen Zulassung durch die Landesanstalt für Ernährung als **hoheitliche** Aufgabe durch. Meine Kontrollkompetenz ist daher gegeben.

Folgende datenschutzrechtliche Verbesserungen habe ich vorgeschlagen:

Datenschutzrechtliche Erklärung

Von Verbänden getragene Kontrollstellen lassen die Landwirte eine datenschutzrechtliche Erklärung unterschreiben, wonach diese den Kontrollstellen gestatten, Daten, die anläßlich der Durchführung der Kontrolle des landwirtschaftlichen Betriebes gespeichert wurden, auch für Zwecke des jeweiligen **Verbandes** zu verwenden (etwa zur Kontrolle nach Verbandsrichtlinien). Ich habe empfohlen, zu überprüfen, ob die Erklärung alle vorgesehenen Datennutzungen umfaßt, damit die Landwirte über alle vorgesehenen Benutzungen ihrer Daten unterrichtet sind.

Meldebogen

Die Betriebe erhalten Meldebögen, in die alle für die Kontrolle maßgeblichen Daten vom Betriebsinhaber einzutragen sind. Ein Meldebogen enthielt sowohl Fragen, die für die Kontrolle nach der EG-Verordnung, als auch **zusätzliche Fragen,** die nur für die Kontrollen nach Verbandsrichtlinien notwendig sind. Es werden aber auch landwirtschaftliche Betriebe kontrolliert, die sich nicht nach den Verbandsrichtlinien kontrollieren lassen, sondern sich **nur** einer Kontrolle **nach der EG-Verordnung unterziehen.** Damit diese Betriebe nicht veranlaßt werden, die zusätzlichen Fragen nach den Verbands-Richtlinien zu beantworten, muß im Meldebogen deutlich sichtbar sein, welche Fragen nur für die Kontrolle nach der EG-Verordnung und welche Fragen zusätzlich für Verbandszwecke erforderlich sind.

Einschaltung einer Anerkennungskommission

In den Verträgen einer Kontrollstelle ist vorgesehen, daß sich die Landwirte bei der Kontrolle des ökologischen Landbaus und der entsprechenden Kennzeichnung der landwirtschaftlichen Erzeugnisse den Entscheidungen einer Anerkennungskommission unterwerfen. Dabei gelangen den Mitgliedern der Kommission personenbezogene Daten des Betriebes zur Kenntnis. In der EG-Verordnung selbst und in den Durchführungsbestimmungen des Ministeriums ist jedoch nicht die Entscheidung einer Anerkennungskommission vorgesehen, sondern die Entscheidung der Kontrollstelle selbst. Die Anerkennungskommission kann nur als Verbandsgremium auftreten. Ich habe daher empfohlen, Verträge über die Kontrolle so zu ändern, daß sich die Landwirte den Entscheidungen der EG-Kontrollstelle unterwerfen. Daten von Betrieben, die nur EG-Kontrolle vereinbart haben, dürfen der Anerkennungskommission lediglich in **anonymisierter Form** übermittelt werden.

14. Schulwesen

14.1 Prüfungen

Im Berichtszeitraum habe ich zwei staatliche Schulämter und ein Gymnasium datenschutzrechtlich überprüft. Es ergaben sich nur geringe Beanstandungen.

1. Staatliche Schulämter

1.1 **Lehrerkartei**

Bei beiden Schulämtern enthielt die **Lehrerkartei** auch Daten, die zur Aufgabenerfüllung nicht erforderlich sind.

So wurden in einem Schulamt die Daten Eheschließung, Name und Geburtstag des Ehegatten bzw. der Kinder, alleinstehende Lehrkraft seit ... erhoben, im anderen Fall der Beruf des Ehegatten. Diese Daten sind zur rechtmäßigen Erfüllung der dem Schulamt zugewiesenen Aufgaben nicht erforderlich. Die Erhebung und Speicherung in der Lehrerkartei sind deshalb unzulässig. Die Daten sind zu löschen.

Soweit die Karteikarten nicht bereits in verschließbaren Karteikästen aufbewahrt werden, sind die Karteikästen abends wegzusperren.

1.2 **Personalblatt**

Für Fragen des Personaleinsatzes führte ein Schulamt für jeden Lehrer ein sogenanntes Personalblatt, das zum Personalnebenakt des jeweiligen Lehrers genommen wird. Es enthält mehrere Datenfelder, die zur Aufgabenerfüllung nicht erforderlich sind. So wird nach dem Geburtsort, dem Familienstand (ledig, verheiratet, verwitwet, geschieden seit), dem Geburtsdatum und Beruf des Ehegatten und der privaten Telefonnummer gefragt.

Im Einvernehmen mit dem Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst vertrete ich dazu folgende Auffassung:

Als Maßstab für den Umfang der zulässigen Datenerhebung können die im staatlichen Schulverwaltungsprogramm SVS gespeicherten Datenarten herangezogen werden. Das Kultusministerium hat bei Einführung dieses Programms zusammen mit dem Hauptpersonalrat genau überprüft, welche Angaben zur Person des Lehrers für die Arbeit des Schulamtes von Bedeutung sind.

Die Angabe des Geburtsortes ist für das Schulamt nicht erforderlich.

Für das SVS wird lediglich erhoben, ob die Lehrkraft verheiratet oder nicht verheiratet ist. Sofern sie nicht verheiratet ist, ist die Angabe des Familienstandes ledig/verwitwet/geschieden freiwillig. Keinesfalls erhoben wird das Datum der Verehelichung, des Todes des Ehegatten oder der Scheidung. Die Angabe des Namens und Vornamens des Ehepartners ist freiwillig; nicht erhoben werden Geburtsdatum und Beruf.

Hinsichtlich der Kinder ist es für die Aufgaben des Schulamtes nur erforderlich, deren Zahl und das Geburtsdatum des jüngsten Kindes (Art. 86 a BayBG) zu kennen, alle weiteren Angaben sind überflüssig.

Der private Telefonanschluß der Lehrkraft sollte nur auf einer freiwilligen Angabe beruhen.

Ich habe dementsprechend eine Überarbeitung des Formblattes gefordert.

1.3 **Fragebogen zum Schulbesuch des Schulrates**

Der Fragebogen wird bei einem Unterrichtsbesuch des Schulaufsichtsbeamten dem zu beurteilenden Lehrer vorgelegt, um nähere Informationen über Umfeld und Interessen des Lehrers zu erhalten. Entgegen Art. 16 Abs. 2 Bayer. Datenschutzgesetz (BayDSG) enthält der Fragebogen weder einen Hinweis auf die Rechtsgrundlage der Datenerhebung noch auf die Freiwilligkeit der Angaben. Häufig ist es für die Lehrkraft von Vorteil, wenn sie sich zu den einzelnen Aspekten einer Beurteilung äußern und

ihre persönliche Situation schildern kann. Gegen einen solchen Fragebogen ist daher nichts einzuwenden, solange die Fragen einen rein dienstlichen Bezug haben. Aus datenschutzrechtlicher Sicht problematisch sind allerdings Fragen, die auch den privaten Bereich der Lehrkraft berühren.

So ist die Beantwortung von Fragen nach **außerdienstlichem Engagement** freiwillig, worauf in dem Fragebogen ausdrücklich hingewiesen werden sollte.

Die Frage nach den **besonderen schulischen Interessengebieten** hat zwar einen dienstlichen Bezug, betrifft aber strenggenommen nur die Neigungen. Bloße Neigungen eines Beamten gewinnen aber für die dienstliche Beurteilung erst dann eine Bedeutung, wenn sie ihren Niederschlag in entsprechenden Kenntnissen, Fähigkeiten oder Tätigkeiten finden. Die Frage sollte daher anders formuliert werden oder entfallen.

Die Frage nach dem **Gesundheitszustand** sollte entfallen. Der Beamte ist nicht verpflichtet, genauere Angaben hierzu zu machen. Zwar enthält die dienstliche Beurteilung auch eine Bemerkung über den Gesundheitszustand des Beamten und damit seine dienstliche Belastbarkeit; da sich einschränkende Angaben der Lehrkraft sowohl zu ihren Gunsten als auch zu ihren Lasten auswirken können, sollte ihr eine solche Auskunft nicht abverlangt werden. Der Beurteilende hat sich hier auf die allgemein bekannten, insbesondere aktenkundigen Tatsachen (z.B. Fehlzeiten) zu verlassen.

Auch in diesem Fall habe ich eine Überarbeitung des Formulars gefordert.

2. Gymnasium

2.1 **Karteien**

In der sogenannten **Schülerkartei** sind auch Daten über ausgeschiedene Schüler enthalten. Die Karteien werden nach Auskunft des Schulsekretariatsleiters von Zeit zu Zeit für Bestätigungen über den Schulbesuch gebraucht. Aussortierungen sind bisher nicht erfolgt.

Eine Regelung zur Aufbewahrung derartiger Karteien besteht nicht.

Ich habe deshalb das Staatsministerium gebeten, eine angemessene Aufbewahrungsfrist festzusetzen.

2.2 **Datenübermittlungen**

Die Daten der Schüler der 5. Jahrgangsstufe werden an das Gesundheitsamt zur Reihenuntersuchung übermittelt. Hierbei handelt sich um eine zugelassene Datenübermittlung. Rückmeldungen über evtl. Gesundheitsmängel erhalten die Eltern.

Die Feststellung einer **Behinderung,** die der Schularzt bestätigt, wird zum Schülerakt genommen. Sie ist erforderlich zur Begründung von evtl. Befreiungen vom Sportunterricht, Prüfungserleichterungen usw.

Bei **psychologischen Problemen** besteht für den Schüler die Möglichkeit, den schulpsychologischen Dienst in Anspruch zu nehmen. Die Schule führt hierüber keinerlei Unterlagen.

Eine Tageszeitung fordert jährlich die **Namen der Abiturienten** an, die dann schulweise in der Zeitung veröffentlicht werden. Die geprüfte Schule hat die Daten bisher zur Verfügung gestellt.

Ich halte die Datenübermittlung nicht durch Art. 62 Bayerisches Erziehungs- und Unterrichtsgesetz gedeckt.

Nach Abs. 2 ist eine Weitergabe von Schülerdaten an außerschulische Stellen nur zulässig, soweit ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird.

Auch Abs. 3, welcher den Datenumfang in einem von der Schule herausgegebenen Jahresbericht regelt, halte ich nicht für analog anwendbar, da der Adressatenkreis eines Jahresberichts regelmäßig kleiner sein wird, als bei Veröffentlichung in einer Tageszeitung.

Das Kultusministerium hat dieser Ansicht zugestimmt. Es hält zumindest eine formlose Zustimmung der betroffenen Schüler für erforderlich.

14.2 Einsicht in Schülerdaten

Zur Problematik der Einsichtnahme von Lehrern in Schülerdaten habe ich mit Unterstützung des Datenschutzbeirates das Bayer. Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst gebeten, ein Gesamtkonzept über die sinnvolle Aufbewahrung von Noten und anderen personenbezogenen Schülerdaten an den einzelnen Schulen zu entwickeln.

Dieses Konzept liegt mir nunmehr vor. Es sieht folgende Einsichtsrechte der Lehrer vor:

Schülerakt:

Zum Schülerakt gehören neben den Grundangaben zum Schüler die Zeugnisentwürfe und alle sonstigen den einzelnen Schüler betreffenden Vorgänge, wie z.B. Urkunden, Bescheinigungen, Schriftwechsel, Nachweise über Ordnungsmaßnahmen usw.

Zur Einsichtnahme sind neben den Erziehungsberechtigten bzw. dem volljährigen Schüler alle Lehrer einer Schule berechtigt, bei denen ein pädagogisches Interesse besteht. Dazu gehören der Beratungslehrer, die den betreffenden Schüler unterrichtenden oder prüfenden Lehrer sowie die Schulleitung.

Nach der Beendigung des Schulbesuches liegt ein solches Interesse des einzelnen Lehrers in der Regel nicht mehr vor. Das Einsichtsrecht auf Seiten der Schule hat dann nur noch die Schulleitung.

Der Schülerakt ist in einem verschlossenen Stahlschrank oder ähnlich gesichert aufzubewahren. Die Schulleitung stellt in jedem Einzelfall sicher, daß nur der berechtigte Personenkreis Einsicht nehmen kann.

Notenbogen:

Bei mehreren Schularten wie z.B. Gymnasien und Realschulen wird in jedem Schuljahr für jeden Schüler ein Notenbogen angelegt. Aus dem Notenbogen ergibt sich der aktuelle Leistungsstand des Schülers, da jeder Lehrer die Ergebnisse der schriftlichen, mündlichen und praktischen Leistungsfeststellungen einträgt. Daneben enthält der Notenbogen auch Aufzeichnungen über die im Schuljahr getroffenen Disziplinarmaßnahmen (z.B. Verweise).

Während Schülerakten nur im Einzelfall zur Beurteilung herangezogen werden, müssen Notenbögen aufgrund ihrer vielfältigen Funktion grundsätzlich allen Lehrern zur Verfügung stehen. Neben den unterrichtenden Fachlehrern haben aufsichtsführende Lehrer, die Mitglieder des Disziplinarausschusses, die Mitglieder der Klassenkonferenz und die Lehrerkonferenz (Vollversammlung) berechtigten Zugang zu den Notenbögen. Eine Kontrolle einzelner Zugriffe würde eine detaillierte Aufschlüsselung voraussetzen, welcher Lehrer aus welchem Grund im laufenden Schuljahr einen Notenbogen eingesehen hat. Der damit verbundene Aufwand wäre mit dem vorhandenen Verwaltungspersonal einer Schule (Sekretariat) kaum zu bewältigen.

Ich habe aus den genannten Gründen dem vorgelegten Konzept grundsätzlich zugestimmt, das Kultusministerium jedoch gebeten, bei der Unterrichtung der Schulen klar herauszustellen, daß eine Einsichtnahme der Lehrer in Schülerdaten nur zulässig ist, wenn sie im Einzelfall zur Erledigung schulischer Aufgaben erforderlich ist. Eine globale, nicht näher motivierte Einsichtnahme durch die Lehrer scheidet damit aus.

Bemängelt habe ich bei dieser Gelegenheit, daß in Schülerakten Schriftstücke oft jahrelang aufbewahrt werden, die für die Entwicklung eines Schülers überhaupt nicht mehr relevant sind. Das Kultusministerium wurde gebeten, das Gesamtkonzept um entsprechende Ausführungen über den rechtmäßigen Inhalt von Schülerakten zu erweitern. Eine Antwort des Kultusministeriums steht derzeit noch aus.

14.3 Herausgabe von Schuljahresberichten an Schulen für Behinderte und für Kranke

Die Herausgabe von Schuljahresberichten ist eines der wichtigen Instrumente zur Selbstdarstellung einer Schule. Die Auflistung der Klassen und ihrer Schüler zählt dabei zum wesentlichen Bestandteil eines Jahresberichts und ist für Schüler und Eltern von besonderem Interesse. Auch Schulen für Behinderte und für Kranke geben Jahresberichte heraus.

In größerem Maße als bei Gymnasien, Realschulen und Volksschulen kommt dem Namen und der Bezeichnung der Schule für den im Jahresbericht aufgeführten Schüler zusätzliche Bedeutung zu. Aus der Sonderschulform kann auf den sonderpädagogischen Förderbedarf und die damit zusammenhängende Behinderung des einzelnen Schülers geschlossen werden. Durch die Veröffentlichung im Jahresbericht wird die Behinderung eines Kindes einem größeren Personenkreis bekannt, da Jahresberichte oftmals über den eigentlichen Adressatenkreis hinaus in Umlauf sind.

Ich habe das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst deshalb gebeten, bei den genannten Schulformen für die Erziehungsberechtigten die Möglichkeit vorzusehen, einer Aufnahme der Daten ihres Kindes in den Jahresbericht widersprechen zu können. Die Erziehungsberechtigten sollten entsprechend informiert werden. Das Staatsministerium hat dem zugestimmt und eine entsprechende Dienstanweisung erlassen.

14.4 Durchführung von Wissenswettbewerben an Volksschulen

Mir wurde folgender Sachverhalt bekannt:

Ein Kreditinstitut hat mit Zustimmung der Schulleitung an einer Volksschule einen Wissenswettbewerb, der die Schüler zum sparsamen und umweltbewußten Umgang mit Resourcen anregen sollte, durchgeführt. Die Daten der teilnehmenden Kinder wurden anschließend für den Versand von Werbematerial des Kreditinstituts verwendet.

Nach § 69 Abs. 1 Volksschulordnung dürfen Druckschriften in der Schule nur verteilt werden, wenn sie für Erziehung und Unterricht förderlich sind und keine kommerzielle oder politische Werbung enthalten.

Ich habe mich deshalb an das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst gewandt, da mir die hier gewählte Art der Adressenermittlung problematisch erscheint.

Das Staatsministerium hat daraufhin die Schulen angewiesen, sofern sie sich aus überwiegend pädagogischen Gründen entscheiden, an Wettbewerben nichtstaatlicher Stellen mitzuwirken, folgende Voraussetzungen sicherzustellen:

Der Veranstalter hat eine Erklärung abzugeben, daß die aus dem Wettbewerb gewonnenen personenbezogenen Daten nicht zu Werbezwecken verwendet werden, sondern ausschließlich dazu dienen, die Sieger zu benachrichtigen oder etwaige Gewinne zu verteilen.

Der Veranstalter muß außerdem zusichern, daß die Daten nur für die Dauer des Wettbewerbs gespeichert und anschließend gelöscht werden.

Damit wurde eine datenschutzgerechte Regelung gefunden.

14.5 Verwendung von Schülerdaten in Rundschreiben

Ein Gymnasium hatte der zuständigen Bezirksregierung von einem Sachschaden, den ein Lehrer während des Unterrichts verursacht hatte, berichtet.

Die Regierung gab das Antwortschreiben, in dem auch Name und Anschrift der geschädigten Schülerin enthalten waren, in Abdruck allen Gymnasien seines Zuständigkeitsbereichs zur Kenntnis. Das berichtende Gymnasium sah darin zu Recht einen Verstoß gegen datenschutzrechtliche Bestimmungen.

Im Rahmen ihrer Aufsichtspflicht hat die Regierung zwar jederzeit das Recht, die ihr nachgeordneten Dienststellen über ihr bedeutsam erscheinende allgemeine Sachverhalte sowie Verfahrens- und Rechtsfragen zu informieren. Die Kopie des Regierungsschreibens enthielt jedoch auch personenbezogene Daten, nämlich Name und Adresse der Schülerin, die in den Schadensfall verwickelt war. Diese Datenübermittlung war zur rechtmäßigen Erfüllung der Aufsichtspflicht nicht erforderlich und damit unzulässig.

14.6 Hochschulgesetz

Der Bayer. Landtag hat im Berichtszeitraum das Gesetz zur Änderung des Bayer. Hochschulgesetzes verabschiedet. Die Neufassung des Hochschulgesetzes enthält nunmehr eine sehr detaillierte Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung der für die Abwicklung des Studiums benötigten Studentendaten. Erforderlich wurde die Datenerhebungsvorschrift wegen der Novellierung des Hochschulstatistikgesetzes, das am 1. Juni 1992 in Kraft getreten ist. Mit diesem Bundesgesetz wurde die Studentenstatistik von einer Primärerhebung auf eine Sekundärstatistik umgestellt, d.h., die Statistik wird aufgrund der Verwaltungsdaten, die die Hochschulverwaltung für ihre administrativen Zwecke erhebt, erstellt.

Mit der genannten Regelung wurde meine Forderung nach einer bereichsspezifischen Datenerhebungsvorschrift im Hochschulgesetz erfüllt, die ich bereits im meinem 10. Tätigkeitsbericht (Nr. 15.2, Seite 45) erhoben hatte.

15. Archiv und Forschung

15.1 Prüfung eines Staatsarchivs

Bei der Prüfung eines Staatsarchivs waren keine gravierenden Mängel festzustellen. Im einzelnen ergaben sich folgende Beanstandungen:

Im Archiv, das nach aktenabgebenden Behörden geordnet ist, wird für die von den Behörden abgegebenen Personalakten eine eigene **Personalaktenkartei** geführt. Diese Kartei, mit deren Hilfe die archivierten Personalakten erst gezielt erschlossen werden können, ist nach dienstlicher Anordnung in einem Nebenraum des Lesesaals in verschließbaren Stahlschränken aufzubewahren. Bei der Prüfung zeigte sich jedoch, daß die Personalaktenkartei für eine Polizeidirektion **nicht abgeschlossen** war.

Im Nebenraum des Lesesaals befinden sich auch die **Repertorien** für jede Behörde. In den Repertorien sind die einzelnen archivierten Vorgänge aufgelistet. In den größtenteils **allgemein zugänglichen** Repertorien wurden sensible personenbezogene Angaben vorgefunden, so beispielsweise ein Abgabeverzeichnis eines Amtsgerichts mit den **Namen von Verurteilten** sowie Grund und Jahr des Strafverfahrens aus der Zeit von 1937 bis 1940.

Ich habe gefordert, daß die Personalaktenkartei und die Repertorien wegen der bestehenden archivrechtlichen Schutzfristen verschlossen zu halten sind, damit eine unbefugte Kenntnisnahme der betroffenen Personen unterbleibt. In den genannten Beispielen kann nicht ausgeschlossen werden, daß einzelne Betroffene dieser Vorgänge noch leben.

15.2 Fotodokumentation eines Stadtarchivs

Ein Bürger hat angefragt, unter welchen Voraussetzungen es zulässig sei, Bildmaterial zu veröffentlichen, das von einem Fotoatelier auf ein städtisches Archiv übergegangen sei. Ferner wollte er wissen, ob er einen Herausgabeanspruch der ihn betreffenden Negative geltend machen könne.

Im Einvernehmen mit der Generaldirektion der staatlichen Archive vertrete ich dazu folgende Auffassung:

Gemäß § 44 Abs. 2 Urheberrechtsgesetz (UrhRG) erwirbt der neue Eigentümer von Lichtbildern bzw. Lichtbildwerken auch das Recht, diese auszustellen. Zu beachten ist aber § 22 Kunsturhebergesetz (KUG). Danach dürfen Bildnisse, die nicht unter die Ausnahmebestimmungen des § 23 KUG fallen, etwa über Personen der Zeitgeschichte, nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Unter Verbreitung im Sinne des KUG ist auch (anders als im UrhRG) die Vorlage im kleinen Kreis gemeint. Fotomaterialien der in Frage stehenden Art dürfen also **bis zum Ablauf von 10 Jahren nach dem Tode des Abgebildeten nur mit Einwilligung** entweder des Abgebildeten oder seiner Angehörigen verbreitet werden. Ein Abgebildeter kann auch gemäß § 37 und § 38 KUG entweder die Vernichtung oder die Übergabe des ihn betreffenden Fotos verlangen.

Die landesrechtlichen Vorschriften des Bayerischen Archivgesetzes treten hinter die Vorschriften des KUG zurück. Eine Vorlage von Bildern ohne Einwilligung der Betroffenen ist demnach auch nicht möglich, wenn dies, wie in Art. 10 Bayerisches Archivgesetz vorgesehen, für eine wissenschaftliche Arbeit zwingend erforderlich ist. Ausnahmen sind nur dort denkbar, wo die betroffene Person durch diese Veröffentlichung zu einer „relativen Person der Zeitgeschichte" wird.

16. Umweltfragen

16.1 Videoüberwachung eines öffentlichen Gehweges vor einem Wertstoffhof

Eine Gemeinde bat mich zu überprüfen, ob gegen die Überwachung eines öffentlichen Gehweges vor einem Wertstoffhof durch eine Videokamera zur Vermeidung von unerlaubten Müllablagerungen datenschutzrechtliche Bedenken bestehen. Nach Auskunft der Gemeinde werden trotz angebrachter Hinweisschilder immer wieder große Mengen von Müll auf dem Gehsteig vor dem Wertstoffhof abgelagert.

Zur Vermeidung unerlaubter Müllablagerungen halte ich die Überwachung des Gehsteiges vor dem Wertstoffhof durch eine Videokamera für zulässig, wenn folgende Grundsätze beachtet werden:

- Die Überwachung ist auf den von illegalen Müllablagerungen betroffenen Bereich zu begrenzen.
- Auf die Videoüberwachung ist durch **Hinweisschilder** aufmerksam zu machen, so daß die Datenerhebung durch die Videokamera soweit wie möglich mit Kenntnis der Betroffenen und nicht heimlich erfolgt. Dieser Hinweis dient damit auch der Vorbeugung.
- Sofern keine unerlaubten Müllablagerungen festzustellen sind, dürfen die 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.

17. Verkehrswesen

17.1 Änderung des Straßenverkehrsgesetzes

Das Bundesministerium für Verkehr hat einen Referentenentwurf zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze vorgelegt.

1. **Verwendung von VZR-Daten für Verkehrs- und Grenzkontrollen**

   Nach dem Entwurf erhalten die **Polizeibehörden** zu Verkehrs- und Grenzkontrollen **Zugriff auf den gesamten Bestand des Verkehrszentralregisters,** also nicht nur auf die im Zentralen Verkehrsinformationssystem (ZEVIS) gespeicherten sog. negativen Fahrerlaubnisdaten (Entziehung, Versagung etc.), sondern auch auf die **Eintragungen von Entscheidungen der Strafgerichte** wegen Straßenverkehrsdelikten, Entscheidungen wegen Ordnungswidrigkeiten im Zusammenhang mit dem Straßenverkehr oder Einstellungen von Verfahren wegen Verkehrsstraftaten nach § 153 a und § 153 b der Strafprozeßordnung (wegen geringer Schuld).

   Diese zusätzlichen Informationen sind zur polizeilichen Aufgabenerfüllung erforderlich,

   - damit die Grenzpolizei feststellen kann, ob einreisende **ausländische Lastkraftwagenführer** bereits wegen Verkehrsverstößen in Erscheinung getreten sind. Diese Feststellungen können dann bei der Entscheidung über eine evtl. Einreiseverweigerung herangezogen werden. Die Bereitstellung dieser Informationen dient der **Erhöhung der Verkehrssicherheit,** die durch diesen Personenkreis immer wieder erheblich gefährdet wird.
   - um bei **Verkehrskontrollen** erforderliche und angemessene Entscheidungen im Einzelfall (z.B. Unterbindung der Weiterfahrt) zu erleichtern.

   Gegen die Online-Verwendung der Eintragungen im VZR für die Verkehrs- und Grenzkontrollen bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

   Daß es zur Bereitstellung und Verwendung solcher Daten für selbstverständliche legitime polizeiliche Zwecke vorher der Änderung des Straßenverkehrsgesetzes bedarf, ist ein weiterer Beleg dafür, wie perfektionistisch und detaillistisch dieses Gesetz 1987 unter dem Eindruck des VZ-Urteils ausgestaltet worden ist.

2. **Verwertung von Protokolldaten zur Verbrechensverhütung und -bekämpfung**

   Nach dem Entwurf dürfen die Aufzeichnungen, die bei einem Abruf im automatisierten Verfahren aus dem Verkehrszentralregister und dem Zentralen Fahrzeugregister in erster Linie zur Datenschutzkontrolle angefertigt wurden, zur Aufklärung oder Verhütung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person verwendet werden, wenn die Aufklärung oder Verhütung ohne diese Maßnahme aussichtslos oder wesentlich erschwert würde.

   Einige Datenschutzbeauftragte lehnen diese Regelung als unverhältnismäßig ab. Es ist jedoch nicht nachvollziehbar, aus welchen überwiegenden datenschutzrechtlichen Gründen unter den genannten strengen Voraussetzungen die Verwertung von Protokolldaten unzulässig sein sollte. Der Schutz der überragenden Rechtsgüter Leib, Leben und Freiheit rechtfertigt die Nutzung der Protokolldaten zur Verbrechensverhütung und -bekämpfung, zumal die Verwendung der Protokolldaten nur bei **schwerwiegenden** Straftaten und auch nur dann zulässig sein soll, wenn die Aufklärung oder Verhütung ohne diese Maßnahme **aussichtslos oder wesentlich erschwert** würde.

   In diesem Zusammenhang verweise ich auf Art. 46 Abs. 3 des Bayerischen Polizeiaufgabengesetzes, der bereits die Möglichkeit vorsieht, Protokollbestände, die nach Abfrage im automatisierten Verfahren eingerichtet worden sind, zu Zwecken der Kriminalitätsbekämpfung auszuwerten. Es gibt keinen vernünftigen Grund, Protokolldateien ausschließlich für

Kontrollzwecke vorzuhalten. Datenschutz ist integrierter Bestandteil der Rechtsordnung. Kontrolldaten dürfen nicht tabuisiert und der Verwendung zu anderen Zwecken völlig entzogen werden.

3. **Datenübermittlung an Stellen im Ausland**

Nach dem Entwurf dürfen die in den Fahrzeug- und Fahrerlaubnisregistern gespeicherten Daten unter bestimmten Voraussetzungen **zur Verfolgung von Straftaten** an Stellen im Ausland übermittelt werden. Nach der derzeit noch gültigen Regelung dürfen Fahrzeugdaten und Halterdaten nur zur Verfolgung von Straftaten, die im Zusammenhang mit der Teilnahme am Straßenverkehr begangen wurden, an ausländische Stellen übermittelt werden.

Die Datenübermittlung an ausländische Stellen erfolgt zur Erfüllung von Verpflichtungen der Bundesrepublik Deutschland aus multilateralen oder bilateralen Vereinbarungen mit anderen Staaten oder zur Durchführung von Rechtsakten der Europäischen Union.

Der Wegfall der Einschränkung ist auch sachgerecht, weil Auskünfte aus den o.b. Registern zur Strafverfolgung erforderlich sein können, ohne daß eine Begehung im Zusammenhang mit einer Teilnahme am Straßenverkehr vorliegt. Dies gilt insbesondere für den Bereich des **organisierten Autodiebstahls.** Bei der Bekämpfung dieser weit verbreiteten Form der organisierten Kriminalität ist gerade auch angesichts des Wegfalls der Grenzen und damit der Kontrollen innerhalb der EU eine Zusammenarbeit der zuständigen Stellen der verschiedenen Länder erforderlich, die auch die Möglichkeit der Datenübermittlung aus den bestehenden Fahrzeug- und Fahrerlaubnisregistern einschließen muß.

4. **Zentrales Fahrerlaubnisregister**

Der Entwurf sieht die Einrichtung eines Zentralen Fahrerlaubnisregisters beim Kraftfahrt-Bundesamt in Flensburg vor. In diesem Register sollen **alle Inhaber von Fahrerlaubnissen und Führerscheinen** gespeichert werden. Weiter soll eine neue Rechtsgrundlage für die bestehenden örtlichen Fahrerlaubnisregister, die bisher in § 10 Abs. 2 StVZO geregelt sind, geschaffen werden.

Die Einrichtung eines Zentralen Fahrerlaubnisregisters dient zunächst dem **Bürger,** der sich bei Kontrollen, bei denen er keinen Führerschein vorweisen kann, Unannehmlichkeiten und Zeitverluste dadurch erspart, daß durch eine Online-Anfrage beim Kraftfahrt-Bundesamt, die rund um die Uhr sowie an Sonn- und Feiertagen möglich ist, seine Fahrberechtigung sofort festgestellt werden kann. Ein automatisiertes zentrales Verzeichnis aller Führerscheininhaber ist desweiteren für die Polizei ein notwendiges Instrument zur **zuverlässigen Feststellung** der Fahrerlaubnis bei einer Kontrolle im Einzelfall an Ort und Stelle. Es trägt zur Verkehrssicherheit bei und ermöglicht sachgerechte Entscheidungen vor Ort.

Die Einführung eines Zentralen Fahrerlaubnisregisters ist auch aufgrund der Entwicklung in der Europäischen Union (Aufhebung der Kontrollen an den Binnengrenzen, vollständiger Wegfall der Umtauschpflicht für die in einem EU-Mitgliedsstaat ausgestellten Führerscheine) erforderlich. Die **2. EG-Führerscheinrichtlinie** enthält deshalb auch die Verpflichtung zu einem effektiven gegenseitigen Informationsaustausch über die bestehenden Fahrerlaubnisse und die ausgestellten Führerscheine. Dieser wäre nicht gewährleistet, wenn sich Behörden der Mitgliedsstaaten durch die 743 örtlichen Führerscheinregister durchfragen müßten. Die übrigen EU-Staaten haben bereits Zentrale Führerscheinregister oder sind dabei, solche zu errichten.

Im übrigen vermag ich eine Gefährdung des allgemeinen Persönlichkeitsrechts durch die Speicherung des **positiven** Umstands der Fahrerlaubnis nicht zu erkennen. Da im Zentralen Fahrerlaubnisregister die Anschrift der Fahrerlaubnisinhaber nicht erfaßt wird, kann dieses auch nicht als zentrales Melderegister benutzt werden.

Die Bedenken einiger Datenschutzbeauftragter gegen ein Zentrales Fahrerlaubnisregister können daher allenfalls aus einer **allgemeinen Technikangst** resultieren, nicht aber aus einer Gefährdung des informationellen Selbstbestimmungsrechts, die auch nicht im entferntesten erkennbar ist.

17.2 Zulassungsrechtliche Behandlung total beschädigter Kraftfahrzeuge

Ein Schwerpunkt der **organisierten Kriminalität** sind der Diebstahl und die Verschiebung von Kraftfahrzeugen. Staatsanwaltschaft und Polizei sind dabei vermehrt mit der Verfolgung von Straftaten befaßt, die zumeist nach folgendem Muster ablaufen:

Die Täter kaufen Schrottfahrzeuge nebst dazugehörigem Kfz-Brief auf, entwenden identische, meist hochwertige Kraftfahrzeuge und bringen an diesen entwendeten Fahrzeugen die Fahrzeugidentifizierungsnummern (FIN) der Schrottfahrzeuge an. Die Fahrzeuge werden sodann ins Ausland verschoben, häufig aber auch in der Bundesrepublik Deutschland zugelassen und zum Teil an gutgläubige Dritte weiterverkauft. Daneben sind Fälle bekannt geworden, in denen das manipulierte Fahrzeug, nachdem eine Vollkaskoversicherung abgeschlossen wurde, als gestohlen gemeldet, ins Ausland exportiert und dort verkauft wurde. Im Inland wurde die Versicherungsleistung kassiert.

Bei den Überlegungen, auf welche Weise die geschilderten Formen der organisierten Kriminalität wirksamer bekämpft werden können, spielen die Datenübermittlungen nach dem sog. „Essener Modell" eine wichtige Rolle: Danach melden die Kasko-Versicherungen ihnen

gemeldete, verkehrsunfallbedingte schwere Schäden an einem Fahrzeug durch Übersendung der Sachverständigengutachten an die Zulassungsstellen weiter. Die Zulassungsstellen können diese Daten nach § 3 Abs. 2 Nr. 11 der Fahrzeugregisterverordnung speichern und der Polizei zur Verfolgung von Straftaten übermitteln (§ 35 Abs. 1 Nr. 2 i.V.m. § 32 Abs. 2 des Straßenverkehrsgesetzes).

Der Bundesbeauftragte für den Datenschutz hat Zweifel geäußert, ob die generelle Übermittlung von Sachverständigengutachten an die Zulassungsstellen für deren Aufgabenerfüllung nach § 17 StVZO erforderlich sei. Er sah in der Zusendung der Schadensgutachten eine Datenerhebung, für die es an einer Rechtsgrundlage fehle. Außerdem äußerte er die Befürchtung, daß die Zulassungsstellen durch diese Direktinformation gegenüber den Eigentümern bzw. Haltern von Kraftfahrzeugen einen Informationsvorsprung erhalten könnten, der ihnen nicht zukomme, und daß dadurch das informationelle Selbstbestimmungsrecht der Betroffenen verletzt werden könnte. Er erwartete, daß ich gegen die Praxis der Behörden einschreite.

Diese Bedenken entbehren nach meiner Auffassung aus folgenden Gründen jeglicher Grundlage:

- Rechtsgrundlage für die Datenübermittlung von den Versicherern an die Kfz-Zulassungsstelle (Übersendung des Schadensgutachtens) ist § 28 des Bundesdatenschutzgesetzes (BDSG). Nach § 28 Abs. 1 Nr. 2 BDSG ist die Datenübermittlung zulässig, soweit sie zur **Wahrung berechtigter Interessen der speichernden Stelle** (hier: des Versicherers) erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt. Die Versicherer dürfen danach zur Vorbeugung und Unterbindung von Autodiebstahl, -hehlerei, und -verschiebung die Kfz-Zulassungsstellen von einem Totalschaden in Kenntnis setzen, um so Schaden von sich und der Versicherungsgemeinschaft abzuwenden. Demgegenüber besteht **kein erkennbares schutzwürdiges Interesse** des betroffenen Kfz-Halters an der Unterlassung der Datenübermittlung vom Versicherer an die Zulassungsstelle.

  Die Datenübermittlung an die Zulassungsstellen ist außerdem nach § 28 Abs. 2 Nr. 1 a BDSG zulässig. Nach dieser Vorschrift dürfen Daten u.a. übermittelt werden, soweit es zur **Wahrung öffentlicher Interessen** erforderlich ist. An der Bekämpfung des organisierten Autodiebstahls und Versicherungsbetrugs besteht ein überragendes öffentliches Interesse. Die Meldungen über Totalschäden – auch und gerade soweit sie Sachverständigengutachten enthalten – stellen eine wichtige Informationsquelle für die Strafverfolgungsbehörden bei der Bekämpfung dieser weitverbreiteten Form der organisierten Kriminalität dar.

- Die Speicherung der Gutachten über total beschädigte Fahrzeuge bei den Zulassungsstellen erfolgt im Rahmen der Aufgabenerfüllung dieser Stellen. Nach § 17 StVZO haben die Kraftfahrzeugzulassungsstellen zur Gewährleistung der Verkehrssicherheit ggf. die dort genannten Anordnungen zu treffen, wenn ein Kfz nicht den Vorschriften der Straßenverkehrsordnung entspricht. Die Zulassungsstellen dürfen die Schadensgutachten zu total beschädigten Fahrzeugen danach zur Prüfung verwenden, ob ein total beschädigtes Fahrzeug abgemeldet wird bzw. im Fall einer Reparatur die vergebene Fahrzeugidentifizierungsnummer zu dem vorgefahrenen Fahrzeug gehört.

- Im übrigen ist die Entgegennahme einer Meldung, um die nicht gebeten worden war, keine Datenerhebung seitens der Kfz-Zulassungsstelle. Für die Entgegennahme der Meldung bedarf es daher keiner Rechtsgrundlage.

- Als der Bundesbeauftragte für den Datenschutz schließlich noch bedauerte, daß er seine Bedenken gegen die Praxis von Versicherungswirtschaft und Zulassungsstellen letzteren nicht mitteilen könne, sah ich den Zeitpunkt gekommen, nachdrücklich vor einer **Verunsicherung der Sicherheitsbehörden** durch **völlig mißverstandenen Datenschutz** und vor der **Verkehrung zum Täterschutz** zu warnen.

17.3 Elektronische Erfassung und Überwachung von Straßenbenutzungsgebühren (Road Pricing)

Das Bundesverkehrsministerium plant die Einführung streckenbezogener **Autobahngebühren** für LKW und PKW etwa ab 1998. Wegen der Vielzahl von Ausfahrten und des hohen Verkehrsaufkommens in Ballungsgebieten ist nicht vorgesehen, Mautstellen wie etwa in Frankreich, Italien oder Spanien einzurichten. Vielmehr sollen die Straßenbenutzungsgebühren auf elektronischem Wege eingezogen werden, ohne den Verkehrsfluß zu behindern. Neu in der Diskussion ist gegenwärtig die Überlegung, auch **Innenstädte** in das Gebührensystem mit einzubeziehen. Gedacht ist dabei an ein **Zonensystem,** dessen Befahren entsprechende **Gebühren** verursacht. Die Gebührenerfassung soll mittels Funkübertragung zwischen Fahrzeug und einer Sende- und Empfangseinrichtung an der Straße erfolgen. Getestet werden zwei Verfahren:

- Beim **Postpaid-Verfahren** (Identifizierungssystem) teilt ein im Pkw angebrachtes elektronisches Gerät der Zahlstelle beim Durchfahren eine kodierte Nummer mit. Die angefallenen Gebühren werden vom Konto des Kfz-Halters abgebucht bzw. diesem in Rechnung gestellt. Da bei diesem System die **Fahrzeuge** über das amtliche Kennzeichen **identifiziert** werden und somit die Halter festgestellt werden können, besteht die Gefahr, daß mit den zu Abrechnungszwecken erhobenen Daten ein **Bewegungsprofil** der Autofahrer erstellt werden könnte.

– Beim **Prepaid-Verfahren** (Wertkartensystem) wird die Gebühr von einer „geladenen" Chip-Karte abgebucht (wie beim Telefonieren mit einer Telefonkarte). Dazu wird jedes Kraftfahrzeug mit einem **„Funk"-Gerät** ausgerüstet, das mit einer **Chip-Karte** betriebsbereit gemacht wird. Die Chip-Karte kann z.B. in Tankstellen gekauft bzw. wieder aufgeladen werden. Durchquert ein solchermaßen betriebsbereites Fahrzeug einen Straßenkontrollpunkt, so wird auf dem Funkwege die entsprechende Gebühr von der Chip-Karte abgebucht.

  Die Chip-Karte enthält wie die Telefonkarte **keine personenbezogenen Angaben.** Auch das im Auto angebrachte Funkgerät wäre frei käuflich und nicht einem bestimmten Kraftfahrzeug zuzuordnen. Bei diesem System erfolgt keine Identifikation des Fahrzeugs, solange beim Durchfahren einer Zahlstelle eine ausreichend geladene Chip-Karte benutzt wird und keine Panne auftritt (z.B. weil das Sendegerät defekt ist).

Bei beiden Systemen kann allerdings auf **begleitende Kontrollmaßnahmen** nicht verzichtet werden. Es ist deshalb vorgesehen, sämtliche Kontrollstellen mit Videoeinrichtungen auszustatten. Durchquert ein „Schwarzfahrer" einen Kontrollpunkt, dann wird automatisch ein Beweisfoto angefertigt, das zur Gebührennacherhebung und in einem evtl. folgenden Ordnungswidrigkeitenverfahren gegen den Halter des Fahrzeugs herangezogen werden kann. Zur Identifizierung des Halters soll das auf dem Beweisfoto erkennbare amtliche Kennzeichen des Fahrzeugs herangezogen werden.

Ein weiteres datenschutzrechtliches Problem ergibt sich aus der Frage, in welcher Form die Richtigkeit der Gebührenrechnung und der elektronischen Abbuchung überprüft werden kann (Einzelgebührennachweis). Dem Betroffenen darf die Möglichkeit nicht abgeschnitten werden nachzuprüfen, in welcher Höhe und bei welcher Gelegenheit Abbuchungen von seiner Chip-Karte oder seinem Konto vorgenommen wurden und aus welchen Einzelposten für welche Erfassungen sich seine Gebührenrechnung zusammensetzt.

Die elektronische Abrechnung von Straßennutzungsgebühren greift in das durch Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 Grundgesetz geschützte Recht des Bürgers auf informationelle Selbstbestimmung ein. Einschränkungen dieses Rechts bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben. Dabei ist ein Verfahren zu wählen, das eine Offenbarung personenbezogener Daten nur in dem erforderlichen Umfang zuläßt. Im Gesetz ist weiter der Verwendungszweck der zwangsweise erhobenen Daten bereichsspezifisch präzise zu bestimmen.

Aus der Sicht des Datenschutzes ist deshalb zunächst zu fordern, daß die zur Gebührenabrechnung, Durchführung von Überwachungsmaßnahmen und Verfolgung von Ordnungswidrigkeiten erforderliche Verarbeitung personenbezogener Daten in einem Gesetz geregelt wird, das diesen vom Bundesverfassungsgericht aufgestellten Grundsätzen gerecht wird. Dabei ist besonders darauf zu achten, daß ein Verfahren gewählt wird, bei dem bei einer ordnungsgemäßen Teilnahme am Straßenverkehr **keine Bewegungsbilder** entstehen. Aus der Sicht des Datenschutzes verdient deshalb das Wertkartensystem eindeutig den Vorzug. Über diese grundsätzlichen datenschutzrechtlichen Forderungen hinaus kann zu Einzelheiten des Verfahrens erst dann Stellung genommen werden, sobald diese bekannt sind.

17.4 Kartengestützte Zahlungssysteme im Öffentlichen Nahverkehr

Verfahren, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden, sind auch im Öffentlichen Nahverkehr in Erprobung. Diese Zahlungsweise erfordert die Speicherung personenbezogener Daten. Wie bei der elektronischen Erfassung und Einziehung von Straßenbenutzungsgebühren für LKW und PKW besteht daher auch hier die Gefahr, daß **Bewegungsprofile** der Fahrgäste erstellt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder haben am 26./27. Oktober 1993 in einer Entschließung gefordert, bei der Einführung kartengestützter Zahlungssysteme im Öffentlichen Nahverkehr darauf zu achten, daß Wertkartensysteme eingesetzt werden, bei denen **im voraus** bezahlt wird und die daher **ohne personenbezogene Daten** auskommen. Außerdem sollte im Öffentlichen Nahverkehr weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: der Kauf einer Fahrkarte am Automaten mit Bargeld. Die Entschließung ist in der Anlage zu diesem Tätigkeitsbericht abgedruckt.

17.5 Weitergabe von Kraftfahrzeughalterdaten an ausländische Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten

In Berichtszeitraum war ich mit der Frage befaßt, ob Fahrzeughalterdaten an schweizerische Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten übermittelt werden dürfen.

Rechtsgrundlage hierfür ist § 37 Straßenverkehrsgesetz (StVG). Die Datenweitergabe zur Verfolgung von Verkehrsordnungswidrigkeiten ist danach grundsätzlich zulässig, wenn multi- oder bilaterale Vereinbarungen vorliegen, aus denen sich die Verpflichtung zur Datenübermittlung ergibt.

Mit der Schweiz liegen bilaterale Vereinbarungen vor, wonach sich das Schweizer Zentralpolizeibüro unmittelbar an das Kraftfahrt-Bundesamt, und die schweizerischen Polizeibehörden unmittelbar an die deutschen Polizeibehörden wenden können. Außerdem besteht für die schweizerischen Behörden noch die Möglichkeit, die zuständige deutsche Strafverfolgungsbehörde (hier: Staats-

anwaltschaften) auf dem unmittelbaren Geschäftsweg um Rechtshilfe zu ersuchen; die Staatsanwaltschaften können bei Ordnungswidrigkeiten die Vornahme der Rechtshilfe der deutschen Verwaltungsbehörde übertragen.

17.6 Mitteilung einer Straftat gegen das Betäubungsmittelgesetz an die Führerscheinstelle

Ein wegen Verstoßes gegen das Betäubungsmittelgesetz verurteilter Bürger wurde von der Führerscheinstelle zur Vorlage eines Gutachtens über die Eignung zum Führen eines Kraftfahrzeuges aufgefordert. Der betroffene Bürger bat mich zu prüfen, wie die Führerscheinstelle von seiner Verurteilung erfahren konnte.

Ich habe dem Bürger mitgeteilt, daß die Fahrerlaubnisbehörde, in deren Bezirk der Verurteilte seinen gewöhnlichen Aufenthalt hat, auf der Grundlage der Anordnungen über Mitteilungen in Strafsachen (MiStra) auf dem Dienstweg Kenntnis von Urteilen in Strafsachen wegen Zuwiderhandlungen gegen das Betäubungsmittelgesetz erlangt. Die Fahrerlaubnisbehörde prüft daraufhin u.a., ob wegen der Tat eine Versagung oder Einziehung der Fahrerlaubnis in Betracht kommt.

Gegen die Mitteilungen bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Bis zum Erlaß des in Vorbereitung befindlichen Justizmitteilungsgesetzes können die Anordnungen über Mitteilungen in Strafsachen als ausreichende Grundlage für die Datenübermittlung angesehen werden. Die Mitteilungen sind auch geeignete und erforderliche Maßnahmen zur Gewährleistung der Verkehrssicherheit, weil Verurteilungen nach dem Betäubungsmittelgesetz Anlaß dazu geben können, die Eignung zum Führen von Kraftfahrzeugen zu überprüfen.

17.7 Speicherung von Daten über Drogendelikte „auf Vorrat" bei einer Fahrerlaubnisbehörde

Der Datenschutzbeauftragte eines Landratsamtes bat mich um Überprüfung der bei der Führerscheinstelle geübten Praxis, die Daten, die im Zusammenhang mit Drogendelikten von der Polizei oder der Justiz gemeldet wurden, zu speichern, obwohl die Betroffenen keine Fahrerlaubnis besitzen und auch keinen Fahrerlaubnisantrag gestellt haben.

Mit dem Staatsministerium des Innern vertrete ich dazu die Auffassung, daß die im Zusammenhang mit Drogendelikten von der Polizei oder Justiz übermittelten personenbezogenen Daten bei den **Fahrerlaubnisbehörden** nicht „auf Vorrat" gespeichert werden dürfen.

Die Führerscheinstellen benötigen die oben bezeichneten Daten für Maßnahmen gegen Inhaber einer Fahrerlaubnis oder in anhängigen Antragsverfahren gegenüber Fahrerlaubnisbewerbern. Besitzt ein Betroffener keine Fahrerlaubnis und hat er bisher auch keinen Fahrerlaubnisantrag gestellt, so werden die Belange der Verkehrssicherheit durch das Drogendelikt grundsätzlich nicht berührt. Eine Speicherung der Daten „auf Vorrat" wäre unzulässig.

Ein seltener Ausnahmefall könnte allenfalls dann vorliegen, wenn sich jemand aufgrund seiner Drogenabhängigkeit als ungeeignet zum Führen von Fahrzeugen, die keine fahrerlaubnispflichtigen Kraftfahrzeuge (z.B. Fahrrad) sind, oder von Tieren im Straßenverkehr (z.B. Reitpferd) erweist, und die Verwaltungsbehörde insoweit eine weitere Verkehrsteilnahme untersagen muß. In diesen wenigen Fällen wird dann aber nicht „auf Vorrat" gespeichert, sondern sofort ein Verwaltungsverfahren eingeleitet.

17.8 Zentrales Verkehrsinformationssystem (ZEVIS)

Das automatisierte Abrufverfahren ermöglicht den Polizeibehörden des Bundes und der Länder einen direkten Zugriff auf die Datenbank des Zentralen Verkehrsinformationssystems (ZEVIS) in Flensburg. Die ZEVIS-Datenbank umfaßt den gesamten Bestand der in Deutschland zugelassenen **Fahrzeuge** und deren **Halter** sowie die sogenannten **negativen Fahrerlaubnisdaten** (z.B. Versagung, Entziehung der Fahrerlaubnis).

Bundestag und Bundesrat haben bei der Verabschiedung des Gesetzes zur Änderung des Straßenverkehrsgesetzes vom 28. Januar 1987 die Bundesregierung gebeten, nach 4 Jahren unter Beteiligung des Bundesbeauftragten für den Datenschutz über die Erfahrungen zu berichten, die mit dem durch das Gesetz eingeführten automatisierten Abrufverfahren, der Aufzeichnungspflicht, der Anfrage unter Verwendung von Personalien (P-Anfrage) und der Einsichtnahme in die örtlichen Fahrzeugregister gemacht worden sind.

Der Erfahrungsbericht der Bundesregierung warf eine Reihe datenschutzrechtlicher Fragen auf, zu denen ich Stellung genommen habe:

1. **Verschlüsselung von personenbezogenen Daten im Funkverkehr**

   Halteranfragen von Polizeibeamten (Streifenwagenbesatzungen) bei ZEVIS und die Antworten laufen über die Einsatzzentralen meist per **Funk.** Seit der Freigabe der Breitbandempfänger durch den Bundesminister für Post und Telekommunikation im Jahr 1992 hat die **Gefährdung des polizeilichen Sprechfunks durch fremdes Abhören** stark zugenommen. Eine **Verschlüsselung** von personenbezogenen Daten im Funkverkehr halte ich für notwendig, um zu verhindern, daß die Daten von Unbefugten abgehört und mißbräuchlich verwendet werden. Die Ausrüstung der herkömmlichen Funkgeräte (Analog-Technik) mit Verschlüsselungsgeräten dürfte aber aus finanziellen Gründen nicht vertretbar sein. Deshalb sollte die Umstellung des Funkverkehrs auf ISDN-Funkgeräte forciert werden. Bis dahin sollte wenigstens **von den technischen Möglichkeiten der Sprachverschleierung** Gebrauch gemacht werden. Besonders sensible Informationen sollten statt über Funk sogar nur über Telefon ausgetauscht werden.

2. **Zusatzprotokollierung für alle Online-Abrufe**

   Bei einer ZEVIS-Abfrage bestehen nach dem Straßenverkehrsgesetz mehrere Aufzeichnungspflichten:

   - Von der übermittelnden Stelle sind **bei jedem Abruf** Aufzeichnungen zu führen über die bei der Durchführung der Abrufe verwendeten Daten, den Tag und die Uhrzeit der Abrufe, die Kennung der abrufenden Dienststelle und die abgerufenen Daten (Grundprotokollierung).
   - Für Abrufe aus dem Zentralen Fahrzeugregister unter Verwendung von Fahrzeugdaten sowie für Abrufe aus dem Verkehrszentralregister, das die negativen Fahrerlaubnisdaten enthält, sind über einen vom Kraftfahrt-Bundesamt ausgewählten **Teil der Abrufe** weitere Aufzeichnungen zu fertigen, die sich auf den **Anlaß des Abrufs** erstrecken und die Feststellung der für den Abruf verantwortlichen Person ermöglichen (Zusatzprotokollierung).

     In Bayern wird über die Anforderungen des StVG hinaus in datenschutzrechtlich vorbildlicher Weise nicht nur für einen Teil der Online-Abrufe, sondern **für alle Abrufe** aus ZEVIS eine Zusatzprotokollierung durchgeführt.

     Ich halte die in **Bayern zu 100 % durchgeführte Zusatzprotokollierung** im Interesse einer effektiven Kontrolle im Einzelfall und zur Prävention für notwendig. Sie hat sich als technisch-organisatorisch und mit vertretbarem Aufwand durchführbar erwiesen, aus der Sicht des Datenschutzes bewährt und sollte für die ganze Bundesrepublik eingeführt werden.

3. **Inhalt der Zusatzprotokollierung (Erweiterung der Schlüsselzahlen)**

   Nach der Fahrzeugregisterverordnung ist bei der Zusatzprotokollierung von der abrufenden Stelle der Anlaß des Abrufs unter Verwendung der 6 folgenden Schlüsselzahlen anzugeben:

   1 Bei Überwachung des Straßenverkehrs: keine oder nicht vorschriftsmäßige Papiere oder Verdacht auf Fälschung der Papiere oder des Kennzeichens

   2 Nichtbeachten der polizeilichen Anhalteaufforderung oder Verkehrsunfallflucht

   3 Feststellungen bei aufgefundenen oder verkehrsbehindernd abgestellten Fahrzeugen

   4 Fahndungs-, Grenzfahndungsaktion, Kontrollstelle

   5 Verfolgung von Straftaten oder Verkehrsordnungswidrigkeiten

   6 sonstige Anlässe.

   Diskutiert wird die Frage, ob die Schlüsselzahlen erweitert werden sollten, damit für eine Kontrolle konkretere Angaben zum Anlaß des Abrufs zur Verfügung stehen.

   Meine wiederholten umfangreichen datenschutzrechtlichen Prüfungen der polizeilichen Abfragen haben ergeben, daß die 6 Schlüsselzahlen für eine effektive Kontrolle ausreichend sind. Bedenkt man, daß die Anfragen vielfach von Polizeibeamten vom Einsatzfahrzeug aus erfolgen, so führt die bisherige Differenzierung der Anfragegründe bereits vielfach zur Überforderung der Einsatzbeamten. Es sollte daher eher an eine Vereinfachung als an eine Erweiterung der Schlüssel gedacht werden. Ich habe erhebliche Zweifel, ob durch eine Erhöhung der Schlüsselzahlen die Kontrolle der Zulässigkeit der Abrufe verbessert wird. Bei meinen systematischen Kontrollen der protokollierten ZEVIS-Abfragen haben sich in keinem Fall Probleme bei der Prüfung der einzelnen Abfragen ergeben. Zu jedem geprüften Fall ließen sich der Sachverhalt und der Anlaß der Abfrage nachvollziehen. Letztlich läßt sich die Zulässigkeit der Abfrage nur durch möglichst baldiges zeitnahes Befragen des abfragenden Beamten kontrollieren.

4. **Protokollierung von Abrufen aus den örtlichen Registern**

   Eine Protokollierung von Online-Abrufen der Polizei aus den örtlichen Fahrzeugregistern ist zur effektiven Kontrolle im Einzelfall und aus Gründen der Prävention ebenso erforderlich wie die Protokollierung von ZEVIS-Abfragen. In Bayern findet eine derartige Protokollierung bereits statt.

5. **Vorschalten einer „Ja/Nein" – Abfrage beim Abruf negativer Fahrerlaubnisdaten (F-Anfrage)**

   Der Bundesbeauftragte für den Datenschutz schlägt vor, eine zusätzliche Abfragemöglichkeit (Voranfrage zur Abrufmöglichkeit negativer Fahrerlaubnisdaten) zu schaffen, bei der keine personenbezogenen Daten, sondern lediglich die Tatsache, ob negative Erkenntnisse vorliegen, übermittelt werden. Damit solle verhindert werden, daß der abrufenden Stelle Daten zur Kenntnis gelangen, die sie für ihre Aufgabenerfüllung nicht benötige.

   Eine Voranfrage zur F-Abfrage halte ich nicht für geeignet, überflüssige Übermittlungen zu vermeiden. Erhält nämlich der abfragende Beamte die Auskunft, daß Erkenntnisse vorhanden sind, wird er regelmäßig diese Erkenntnisse zu seiner Aufgabenerfüllung auch benötigen und weitere Abfragen durchführen. Die Voranfrage würde daher nur eine unnötige und überflüssige Mehrarbeit bedeuten.

6. **Zulässigkeit des in Bayern praktizierten sog. „virtuellen Verfahrens"**

   Nach dem Straßenverkehrsgesetz dürfen Anlagen zum Abruf im automatisierten Verfahren nur einge-

richtet werden, wenn gewährleistet ist, daß zur Sicherung gegen Mißbrauch die erforderlichen technischen und organisatorischen Maßnahmen ergriffen werden, insbesondere durch Vergabe von **Kennungen** an die zum Abruf berechtigten **Dienststellen** und die **Datenendgeräte.**

Während im herkömmlichen Verfahren zur ZEVIS-Nutzung jedes Endgerät durch eine eigene Leitung mit dem Rechner des Kraftfahrt-Bundesamtes (KBA) verbunden ist, bedienen sich Bayern und einige andere Bundesländer des sog. **virtuellen Verfahrens.** Bei diesem Verfahren sind die Endgeräte nicht direkt mit dem Rechner des KBA verbunden. Der Dialog Endgerät – KBA erfolgt über einen Großrechner des Landeskriminalamts, der den Abruf für ein bestimmtes Endgerät mit einer bestimmten Kennung beim KBA vornimmt.

In **Bayern** wurden zudem noch seit Ende 1990 größtenteils die bisher üblichen Endgeräte (mit eigener Kennung) durch **Arbeitsplatzsysteme** abgelöst. Für die Arbeitsplatzrechner sind jeweils ZEVIS-Kennungen vergeben, die beim KBA registriert (generiert) sind. Wird mit einem Endgerät ein Abruf durchgeführt, so erfolgt die Identifizierung des Nutzers beim KBA nicht mit einer Kennung dieses Gerätes, sondern mit einer der ZEVIS-Kennungen des gemeinsamen Arbeitsplatzrechners. Da außerdem ein Arbeitsplatzrechner für Endgeräte verschiedener Dienststellen zur Verfügung stehen kann, ist im Einzelfall für das KBA (sehr wohl aber für das LKA) zum Zeitpunkt des Abrufs **nicht immer feststellbar, welche Dienststelle den Abruf** durchgeführt hat. **In solchen Fällen läßt sich die abrufende Dienststelle aber nachträglich aufgrund der hier bei allen Abrufen erfolgenden Protokollierung der abrufenden Person feststellen.**

Der Bundesbeauftragte für den Datenschutz hatte darauf hingewiesen, daß das KBA bei dem virtuellen Verfahren nur die Dienststelle feststellen kann, bei der der Arbeitsplatzrechner steht, jedoch nicht von welchen Dienststellen und von welchen Datenendgeräten letztlich die Abrufe durchgeführt wurden. Damit werde gegen die im Straßenverkehrsgesetz und der Fahrzeugregisterverordnung enthaltenen Regelung zur Sicherung gegen Mißbrauch verstoßen.

Richtig ist, daß in Einzelfällen das KBA erst auf Nachfrage beim LKA feststellen kann, von welcher Dienststelle die Anfrage eingegangen ist. Dies ist der Fall, wenn mehrere Dienststellen an einem gemeinsamen Arbeitsplatzrechner angeschlossen sind. Durch die in Bayern durchgeführte **vollständige** Protokollierung von ZEVIS-Abfragen, die weit über den vorgeschriebenen Rahmen hinausgeht, kann – wie auch der Bundesbeauftragte einräumen muß – in jedem Fall die für den Abruf verantwortliche Person und deren Dienststelle festgestellt werden.

Der Entwurf zur Änderung des Straßenverkehrsgesetzes enthält eine ausdrückliche Regelung für das in Bayern praktizierte virtuelle Verfahren.

Dieser Fall belegt exemplarisch den Überperfektionismus, der in den gesetzlichen (!) Detailregelungen des Straßenverkehrsgesetzes von 1987 in völliger Verkennung des Grundsatzes der Normenklarheit zum Ausdruck gekommen ist. Das Gesetz schreibt eine bestimmte Sicherungsmethode vor, ohne andere bereits vorhandene mindestens gleichwertige Sicherungsvorkehrungen zu berücksichtigen oder Raum zu lassen für eine kostensparende, effektivere behördliche Organisation der Datenverarbeitung. Das ZEVIS-Gesetz von 1987 übertrifft die wegen ihrer perfektionistischen und detaillistischen Regelungen verrufenen EG-Richtlinien bei weitem.

Der Gesetzgeber sollte den Erfahrungsbericht der Bundesregierung zum Anlaß nehmen, das überperfektionistische ZEVIS-Gesetz grundlegend zu vereinfachen und praktikabler zu gestalten sowie der Organisationshoheit der Länder stärker Rechnung zu tragen.

17.9 Zugang zu ZEVIS (Sperrung bei Fehlversuchen)

Das Straßenverkehrsgesetz erlaubt der Polizei für die dort genannten Zwecke den Abruf aus dem Verkehrszentralregister und dem Zentralen Fahrzeugregister des Kraftfahrt-Bundesamtes (KBA) im **automatisierten Verfahren.** Die Einrichtung eines automatisierten Abrufverfahrens ermöglicht der Polizei einen sog. Online-Zugriff auf die gespeicherten Daten. Dies führt allerdings auch dazu, daß die abgebende Stelle (KBA) im Verfahrensablauf keinen Einfluß mehr auf die Datenübertragung hat. Zum Ausgleich dafür ist in der Fahrzeugregisterverordnung festgelegt, daß zur Sicherung gegen Mißbrauch durch ein **selbsttätiges Verfahren** zu gewährleisten ist, daß keine Abrufe erfolgen können, wenn der abgebenden Stelle die Kennung des Endgerätes nicht bekannt ist oder die Benutzerkennung und das Paßwort des Abrufenden **mehr als zweimal hintereinander unrichtig eingegeben** wurden. Wie ich bereits im 14. Tätigkeitsbericht ausgeführt habe, entspricht das derzeit in Bayern praktizierte Verfahren nicht dem Sinn und Zweck dieser Vorschrift, im Interesse der Datensicherheit die Zahl der folgenlosen Fehlversuche zu begrenzen.

Im Berichtszeitraum habe ich mich wegen dieser Mängel erneut an das Innenministerium gewandt. Mir wurde zugesagt, daß im Zusammenhang mit dem geplanten Wechsel auf neue Betriebssystemversionen die geforderten Funktionen verwirklicht werden sollen.

17.10 Mißbrauch von ZEVIS-Abfragen zur Kraftfahrzeugverschiebung

Im Berichtszeitraum wurden mir aufgrund von Presseberichten zwei Fälle bekannt, in denen der Verdacht der

mißbräuchlichen Abfrage im Zentralen Verkehrsinformationssystem (ZEVIS) durch Polizeibeamte besteht:

1. In einem Fall stellte ein Polizeibeamter durch ZEVIS-Anfragen die Fahrgestellidentifikationsnummern (FIN) von Fahrzeugen fest, die von Kriminellen zur Entwendung vorgesehen waren. Der Polizist gab die Nummern an den Beschäftigten einer Autofirma weiter, der damit die Schlüssel-Code-Nummer der Fahrzeuge ermitteln und Nachschlüssel fertigen konnte. Mit den Nachschlüsseln wurden dann die Fahrzeuge von der Straße weg entwendet.
2. Ein weiterer Polizeibeamter soll über den Dienstcomputer Halterdaten von Fahrzeugen abgefragt haben, für die sich mutmaßliche Autoschieber interessierten. Das Strafverfahren ist noch nicht abgeschlossen.

Aufgrund dieser Vorkommnisse habe ich das Innenministerium um Auskunft gebeten, welche Maßnahmen bei der bayerischen Polizei getroffen wurden, um derartige Mißbrauchsfälle, die der organisierten Kriminalität zuzurechnen sind, künftig zu verhindern.

Das Innenministerium hat mir mitgeteilt, daß sich ein Datenmißbrauch durch einzelne Bedienstete, selbst mit besten Sicherungsmaßnahmen nicht völlig ausschließen lasse. Die in Bayern bestehenden Zugriffssicherungen würden in erheblichem Maße zum Schutz vor Mißbräuchen beitragen. In der Vergangenheit habe sich gezeigt, daß mit der Aufzeichnung der Datenabrufe Verdachtsfälle unbefugter Datennutzung schnell nachgewiesen oder ausgeräumt werden konnten. Es gäbe nach den vorliegenden, auf dienstaufsichtlichen Überprüfungen beruhenden Erkenntnissen und der geringen Anzahl der festgestellten Verstöße gegen die Datenschutzbestimmungen keinen Zweifel daran, daß die datenschutzrechtlichen Vorschriften von der Polizei in weitestgehendem Umfang eingehalten würden. Gravierendes Fehlverhalten einzelner Beamter würde die seltene Ausnahme darstellen, die strafrechtlich und disziplinär konsequent geahndet würde.

Ich stimme mit der Beurteilung des Innenministeriums im Grundsatz überein. Ich meine aber, daß die Protokollierung der Anfragen noch stärkere präventive Wirkung gewinnen würde, wenn nicht nur von mir, sondern im verstärkten Maße **auch von den Polizeidienststellen selbst verdachtsunabhängige Kontrollen** der Protokollbestände durchgeführt würden.

18. Medien

18.1 Reality-TV

Im schärfer werdenden Kampf um Einschaltquoten werden seit einiger Zeit auch sogenannte Reality-TV-Sendungen ausgestrahlt. Dabei steht oftmals nicht die Berichterstattung über Katastropheneinsätze und Rettungsversuche im Vordergrund, sondern die Darstellung individueller Lebensschicksale. Eine solche Herausstellung von Personen, die nicht Personen der Zeitgeschichte sind, erscheint **im Blick auf das allgemeine Persönlichkeitsrecht der Betroffenen äußerst bedenklich.**

Bei Sendungen dieser Art muß sichergestellt werden, daß der Datenschutz der Opfer und der Mitwirkenden an Rettungsaktionen gewährleistet ist.

Nach meiner Auffassung enthalten die einschlägigen Rechtsvorschriften (Polizeiaufgabengesetz, Rettungsdienstgesetz, Feuerwehrgesetz, Bayer. Datenschutzgesetz) keine Rechtsgrundlage für die Erhebung personenbezogener Daten durch Angehörige des öffentlichen Dienstes in der Form, daß diese über Einsätze bei Unfällen und Katastrophen Aufzeichnungen für Sendeanstalten anfertigen.

Das Staatsministerium des Innern sieht für die bayerische Polizei eine Möglichkeit zur Mitwirkung **nur in Ausnahmefällen** gegeben. Unterstützungswürdig sollen vor allem sein Berichte über vorbeugende Maßnahmen, Sendungen über Unfälle, die **der Aufklärung von Verkehrsteilnehmern** über das Verhalten am Unfallort dienen können, und Sendungen, welche die **Bereitschaft zur Ersten Hilfe** fördern sollen. Dabei müssen der Datenschutz und die Persönlichkeitsrechte sichergestellt sein. Ähnlich restriktiv hat das Staatsministerium des Innern auch zur Mitwirkung von Feuerwehren und Rettungsdienstorganisationen Stellung genommen. Diese restriktive Haltung begrüße ich.

Im Spannungsfeld von verfassungsrechtlich geschützter Rundfunkfreiheit und schutzwürdigen Belangen der Betroffenen sind jedoch auch die **Rundfunkanstalten und die Landesmedienanstalten** gefordert.

Es bleibt zu hoffen, daß sich die Medien ihrer mit der Rundfunkfreiheit verbundenen Verantwortung bewußt sind und von einer die Menschenwürde verletzenden Berichterstattung Abstand nehmen.

19. Technischer und organisatorischer Bereich

19.1 Technische Grundsatzfragen

19.1.1 Risiken der Informations- und Kommunikationstechnik

In der öffentlichen Verwaltung gibt es heute kaum noch einen DV-freien Bereich. Die maschinelle Datenverarbeitung ist zu einer unverzichtbaren Arbeitshilfe geworden. Dem Einsatz moderner Informations- und Kommunikationstechnik ist es zu verdanken, daß die vom Gesetzgeber gestellten Aufgaben zeitgerecht und kostengünstig bewältigt werden können.

Die heutige Informations- und Kommunikationstechnik bietet sicherlich auch Mißbrauchsmöglichkeiten. Sicherheitsexperten stellen das immer wieder heraus. Durch ihre ständigen Warnungen wollen sie in erster Linie er-

reichen, daß sich der Anwender über einen wirksamen Datenschutz **rechtzeitig Gedanken** macht. Übertriebene Kritik und maßlose Übertreibungen bewirken bei Außenstehenden allerdings eher eine technikfeindliche Haltung in der Gesellschaft und Vorbehalte gegen die notwendige Nutzung der modernen Informationstechnik.

Die moderne Datenverarbeitungs- und Kommunikationstechnik bietet heute allerdings auch **genügend Kontroll- und Revisionsmöglichkeiten,** um ihren ordnungsgemäßen Einsatz weitgehend sicherzustellen. Moderne elektronische Zugangskontrollsysteme, der Einsatz von Verschlüsselungs- und sicheren Authentisierungsverfahren sowie ausgereifte Protokollierungssysteme mit leistungsfähigen Audit-Komponenten seien als Beispiele genannt.

Wie in vielen Lebensbereichen so ist auch in der Informationsverarbeitungs- und Kommunikationstechnik ein gewisses **Restrisiko** in Kauf zu nehmen. Würde man absolute Sicherheit fordern, wäre ein wirtschaftlicher Einsatz dieser Technik nicht mehr möglich. Das kann aber nicht das Ziel eines vernünftigen Sicherheitssystems sein.

Bedauerlich ist allerdings, daß viele Sicherheitseinrichtungen heute noch sehr teuer sind und ihr Einsatz deshalb aus Haushaltsgründen häufig zurückgestellt wird. Viele Sicherheitsmaßnahmen sind außerdem unwirtschaftlich, weil die bekannt gewordenen Mißbrauchsfälle äußerst selten sind. Die häufig zitierten Fälle von Computerkriminalität haben stets finanzielle Hintergründe und betreffen hauptsächlich den Bereich der Privatwirtschaft.

Manche Experten bemängeln, daß Sicherheitskomponenten, die im nachhinein ergriffen werden, teuerer und deshalb für einen breiten Einsatz nicht geeignet seien. Ob allerdings eine von vornherein im System integrierte Sicherheit wesentlich billiger ist und vom Markt angenommen wird, bleibt abzuwarten.

19.1.2 Übertragungssicherheit im Mobilfunk

Im 14. Tätigkeitsbericht habe ich ausführlich darüber informiert, daß das Fernmeldegeheimnis und der Persönlichkeitsschutz durch die Aufhebung der Beschränkung der zulässigen Empfangsbereiche für Rundfunkempfänger zusätzlich gefährdet wurden. Als Reaktion auf diese Bedrohung hat das Bayerische Staatsministerium des Innern seine nachgeordneten Dienststellen angewiesen, durch interne Dienstanweisungen dafür Sorge zu tragen, daß, soweit einsatztaktisch möglich, die Übermittlung sensibler Sachverhalte auf dem Funkweg unterbleibt oder zumindest verringert wird bzw. so erfolgt, daß die von Unbefugten aufgefangenen Erkenntnisse nicht zum Nachteil von Betroffenen genützt werden können.

Die Technische Kommission der Konferenz der Innenminister des Bundes und der Länder hatte zur Gewährleistung der Vertraulichkeit im Funkverkehr zunächst ins Auge gefaßt, einfache Inverter-Bausteine zur Invertierung des Funkverkehrs der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) einzuführen. Dieser Plan mußte jedoch wieder verworfen werden, da Invertierungsdecoder, welche diese Maßnahme unterlaufen, auf dem Markt erhältlich sind und nach der Freigabe der Frequenzbereichsgrenzen legal betrieben werden dürfen, womit weiterhin eine unerlaubte Abhörung des mobilen Funkverkehrs möglich wäre.

Seit Mitte 1992 werden erste digitale Funktelefone im sogenannten D1- (Mobilfunknetz der Telekom) und D2-Netz (Mobilfunknetz der Mannesmann Mobilfunk GmbH) erprobt, die eine permanente Verschlüsselung des Sprechfunks ermöglichen und somit auch gegen den professionellen Abhörer sicher sind. Bis zu einem flächendeckenden Einsatz dieser Geräte dürften aber noch einige Jahre vergehen.

19.1.3 Elektronische Krankenversicherungskarte

In der Krankenversicherung führten 1993 verschiedene Krankenkassen Pilotversuche durch, bei denen anstatt der bisherigen Krankenscheinhefte jedem Versicherten eine Chipkarte ausgehändigt wurde, auf der seine Versichertendaten (Name, Anschrift, Geburtsdatum, Krankenkasse, Versichertennummer, Gültigkeitszeitraum) gespeichert sind.

Damit auf dieser Chipkarte nur zulässige Daten gespeichert werden können, muß durch technische und organisatorische Maßnahmen gesichert werden, daß nur **die Krankenversicherung** als speichernde Stelle Daten auf der Chipkarte speichern kann. Andere Stellen wie Ärzte und Apotheker, welche die auf der Chipkarte gespeicherten Versichertendaten lesen, dürfen die gespeicherten Daten nicht verändern und vor allem keine zusätzlichen Daten speichern.

In Bayern werden die Allgemeinen Ortskrankenkassen Anfang 1994 an alle Mitglieder derartige Chipkarten ausgeben. Damit keine zusätzlichen Daten auf dieser Karte gespeichert werden, wurde die **Speicherkapazität des Chip begrenzt.** Um den Versicherten und dem Arzt die Kontrolle der gespeicherten Daten auf ihre Richtigkeit zu ermöglichen, sind auf der Chipkarte der Name des Versicherten, die Kassennummer, die Versichertennummer und der Gültigkeitszeitraum aufgedruckt. Da man nach der gewählten Technik eine Manipulation der gespeicherten Daten – es gibt heute schon genügend Geräte auf dem Markt, mit deren Hilfe man die im Chip gespeicherten Daten verändern kann – nicht verhindern kann, empfiehlt es sich, bei jedem Lesevorgang die gespeicherten mit den auf der Karte aufgedruckten Daten zu **vergleichen.** Die Mißbrauchsmöglichkeiten sind allerdings nicht größer als beim bisherigen Krankenscheinheft. Schließlich wird in jeder Krankenkasse ein Lesegerät aufgestellt, mit dessen Hilfe der Versicherte die gespeicherten Daten überprüfen kann.

Von der zukünftigen Technik der elektronischen Krankenversicherungskarte ist zu fordern:

- Ein Schreibzugriff ist nur der ausstellenden Krankenkasse zu gestatten (Paßwortschutz).

- Die nicht benötigten Speicherplätze sind zu sperren.
- Es sollten nur amtlich zugelassene Lese- und Schreibgeräte (eventuell mit Prüfzertifikat des Bundesamts für Sicherheit in der Informationstechnik) verwendet werden.

19.1.4 Einsatz von Abfragesprachen

Wurden in der automatisierten Datenverarbeitung Abfragesprachen eingesetzt, so habe ich bei meinen Prüfungen wegen der Mächtigkeit dieser DV-Werkzeuge bisher stets höhere Anforderungen an die technischen und organisatorischen Sicherungsmaßnahmen gestellt als bei üblichen DV-Anwendungsprogrammen.

Die Hersteller von Datenbanksystemen bieten neben dem Datenbankverwaltungssystem mit seiner „Batch-Schnittstelle" zur Datenverarbeitung innerhalb von Anwendungsprogrammen meist auch eine systemspezifische Abfragesprache an, mit der die vom System verwalteten Datenbestände in anwenderfreundlicher Art und Weise **ausgewertet** und **abgefragt** werden können. Mit Hilfe von Abfragesprachen lassen sich sogar physisch getrennte Datenbanken **verknüpfen,** sofern sie vom gleichen System verwaltet werden.

Abfragesprache und Anwendungsprogramm unterscheiden sich hinsichtlich des Zugriffs auf Daten, die von einem Datenbanksystem verwaltet werden, wie folgt voneinander: Im **Anwendungsprogramm,** unabhängig davon ob Batch- oder Dialogprogramm, ist die Art des Datenzugriffs stets im Programm vorgegeben, beispielsweise der Zugriff auf Name, Adresse und Geburtsdatum einer gespeicherten Person zur Feststellung ihrer Identität. Ein Abfragen nach einem anderen ebenfalls in der Datenbank enthaltenen Feld, etwa dem Einkommen, ist in dem skizzierten Beispiel vom Programm her nicht vorgesehen und folglich mit ihm auch nicht durchführbar. Während der Benutzer eines vorgefertigten Programms also nur auf das zugreifen kann, was das Programm zuläßt, kann der Benutzer der **Abfragesprache** im Prinzip auf alle Felder aller vom System verwalteten Datenbanken zugreifen und diese miteinander verknüpfen. Der Benutzer ist damit gleichsam imstande, sein eigenes **Datenzugriffsprogamm** zu formulieren, wobei er dieses ständig seinen neuen Bedürfnissen anpassen kann. Im oben geschilderten Beispiel kann er nach Bedarf zusätzlich beispielsweise auf alle Einkommensdaten und/oder auf alle Sozialdaten zugreifen.

Beim Einsatz von Abfragesprachen ist es auch möglich, bestimmte Datenfelder und Datensätze, ja sogar ganze Datenbanken gegen den Zugriff bestimmter Benutzer zu sperren. Von solchen Einschränkungen macht man in der Praxis allerdings nur ungern Gebrauch, weil dadurch die Möglichkeiten einer frei formulierbaren Abfragesprache stark eingeschränkt werden. Man eröffnet einem Benutzer deshalb entweder die Abfragesprache mit all ihren Möglichkeiten oder man verzichtet ganz darauf, ihm die Berechtigung für die Benutzung der Abfragesprache zu geben, weil man bei der Festlegung der Zugriffsbefugnisse die späteren Anforderungen nicht kennt.

Als Kontrollmaßnahmen beim Einsatz von Abfragesprachen habe ich in der Vergangenheit vorgeschlagen:

- Restriktive Vergabe der Benutzungsberechtigung
- Schriftlicher Antrag für jede Abfrage zur Dokumentation
- Genehmigung jeder Auswertung durch eine dafür autorisierte Person vor ihrer Durchführung (Vier-Augen-Kontrolle)
- Protokollierung der Abfragekriterien, so daß im Nachhinein erkennbar ist, wer wann welche Abfragen getätigt hat
- Bei besonders sensiblen Datenbeständen: Kontrolle jeder Ergebnisliste durch den internen Datenschutzbeauftragten auf unzulässige oder vorher nicht vorhersehbare Selektionen

Seit Jahren setzen die Allgemeinen Ortskrankenkassen für Querschnittsauswertungen ihrer Datenbestände die Abfragesprache SIRON ein. Die AOK Aschaffenburg hat beispielsweise für die Anforderung von SIRON-Abfragen ein übersichtliches Formblatt entwickelt.
Die Ergebnisse solcher Auswertungen können, müssen jedoch nicht personenbezogen sein. Eine besonders sensible personenbezogene Auswertung wäre etwa eine Auflistung aller Personen mit überdurchschnittlichen Arztleistungen, wobei die Versicherten noch einer bestimmten Altersgruppe oder einer bestimmten Einkommensklasse zugehörig sein könnten. Die Auswertungen werden von mir kontrolliert.

19.1.5 Hinweise zu Protokolldateien

Zur Beweissicherung für die ordnungsgemäße Abwicklung von DV-Aktivitäten, für versuchte Zugriffsschutzverletzungen und für Zwecke der DV-Revision zeichnen Betriebs-, Sicherheits- und Anwendungssysteme Benutzungsdaten auf. Diese Protokolldaten sollen Aufschluß darüber geben, wer zu welcher Zeit mit welchen Mitteln und zu welchem Zweck auf welche Daten zugegriffen hat. Oft ist es zweckmäßig, auch die Ressource (Terminal, PC, Bildschirm eines Mehrplatzsystems) zu protokollieren, von der aus eine Aktion gestartet wurde.

Bei besonders sensitiven Anwendungen ist sogar eine lückenlose Erfassung der Benutzeraktivitäten angezeigt. Aus diesem Grunde sind die Protokolldateien gegen einen Zugriff Unbefugter besonders zu schützen. Folgende Maßnahmen sind zu beachten:

- Protokolldateien sind wegen ihrer Zuordenbarkeit zu bestimmten Personen zur Leistungs- und Verhaltenskontrolle der Benutzer des DV-Systems geeignet. Eine rechtzeitige Einbeziehung und Beteiligung der **Personalvertretung** ist deshalb angezeigt.
- In einer **Vereinbarung** mit der Personalvertretung ist festzulegen, welche Daten zu Zwecken der Datenschutzkontrolle, der Datensicherheit und zur Sicherstellung eines ordnungsgemäßen DV-Betriebs protokolliert werden. Eine Änderung der Zweckbestim-

mung ohne Anhörung der Personalvertretung ist auszuschließen.
- Die **zulässigen Auswertungen** der Protokolldateien und die Art ihrer Nutzung sind unter Beteiligung des internen Datenschutzbeauftragten und der Personalvertretung festzulegen.
- Der **Umfang der Protokollierung** ist von der Sensitivität der Anwendung und der Daten abhängig. In belanglosen Fällen dürfte es reichen, wenn man sich auf signifikante Stichproben beschränkt (Grundsatz der Angemessenheit).
- Protokolldaten sind nach einer angemessenen Zeit zu **löschen.** Im allgemeinen genügt es, Protokolldaten für Zwecke der Datenschutzkontrolle für den Zeitraum eines Jahres vorzuhalten.
- Der interne Datenschutzbeauftragte muß eine **Übersicht** führen, aus der hervorgeht, welche Art von Protokolldaten in welchen Verfahren aufgezeichnet werden.

19.2 Prüfungstätigkeit

19.2.1 Kontrolle und Beratung

Ein Schwerpunkt war auch im Berichtszeitraum die Kontrolle der technischen und organisatorischen Datensicherheitsmaßnahmen.

Folgende **Dienststellen** habe ich nach Art. 15 BayDSG (teilweise i.V.m. § 9 BDSG und Anlage) kontrolliert:

- Anstalt für kommunale Datenverarbeitung in Bayern (AKDB), München (Systemverwaltung)
- AKDB, KDZ Landshut
- Bayer. Staatsministerium für Wirtschaft und Verkehr, München
- Betriebskrankenkasse der MAN, Nürnberg
- Bezirk Schwaben, Augsburg
- Bezirksfinanzdirektion Regensburg
- Gemeinde Dietramszell
- Kreiskrankenhaus Fürstenfeldbruck
- Landbauamt München
- Landeshauptstadt München (Rechenzentrum, Einsatz von BS2000 V10.0 mit SECOS)
- Landeskriminalamt München (Zugriffssicherheit der APC-Verfahren)
- Landesversicherungsanstalt Unterfranken, Würzburg
- Landratsamt München
- Landratsamt Traunstein
- Polizeiinspektion Bayreuth-Land (APC-Sicherheit)
- Staatliches Gesundheitsamt Weilheim
- Stadt Garching
- Universität Augsburg (Rechenzentrum)
- Wasserwirtschaftsamt Landshut.

Die Prüfung bei der AKDB München war schwerpunktmäßig auf die Systemverwaltung ausgerichtet.
Im Rechenzentrum der Landeshauptstadt München habe ich mich über die Erfahrungen beim Einsatz von SECOS informiert, einer zusätzlichen Sicherheitssoftware des Herstellers zum Betriebssystem BS2000 V10.0. Prüfungsgegenstand waren die Protokollebene (SAT) und ihre Anwendung für eine effektive Datenschutzkontrolle und DV-Revision. Für den Umfang der Protokollierungen und deren Auswertung im laufenden Betrieb habe ich Vorschläge entwickelt.
Bei der Polizeiinspektion Bayreuth-Land galt mein Interesse dem **Zugriffsschutz** auf gespeicherte Daten und der Protokollierung von Zugriffen, verbunden mit möglichen Systemreaktionen bei unbefugten Zugriffsversuchen im Rahmen des Einsatzes des Betriebssystems SINIX.
Bei der Universität Augsburg prüfte ich die Datensicherheitseinrichtungen im Rechenzentrumsbereich.

Zahlreiche Dienststellen habe ich im Berichtszeitraum beraten. Es ging hauptsächlich um folgende Themenkreise:
- Datenschutz- und Datensicherheitsmaßnahmen bei **Um- oder Neubauten von Amtsgebäuden** (Außenhaut- und Innenraumsicherung),
- Sicherheitsmaßnahmen bei der **Einrichtung von DV-Bereichen** wie Zutrittsschutz, Brand- und Wasserschutz, Entsorgung,
- technisch-organisatorische Hilfestellung bei der **Einführung von DV-Systemen** und beim Einsatz von PC-Systemen (Zugriffsschutz, Datensicherung, Katastrophenvorsorge, Vollständigkeit von DV-Dienstanweisungen, Revisionsfähigkeit der Datenverarbeitung) oder
- Sicherheitsmaßnahmen beim **Aufbau von Netzwerken** (Datensicherheit innerhalb des Netzes, Maßnahmen gegen unbefugtes Eindringen ins Netz).

19.2.2 Ergebnisse der Kontrolltätigkeit

Die Kontrollen zeigten trotz immer schwieriger werdender Haushaltslage das Bemühen der Verwaltung, Maßnahmen zum Datenschutz und zur Datensicherung im gebotenem Maße voran zu bringen. Dabei war insbesondere festzustellen, daß einige Verwaltungen Datenschutz- oder Datensicherheitsmaßnahmen für ihren Zuständigkeitsbereich durch eine Gesamtregelung zu erledigen suchten. Auf diese Weise sind sowohl gleichartige und wiederholte Prüfungsbemerkungen zu vermeiden als auch Finanzmittel einzusparen, soweit Mängel durch Sammelbeschaffungsmaßnahmen erledigt werden konnten.

Als Ergebnis fortschreitender Automatisierung habe ich auch bei kleinen Verwaltungseinheiten (Sachgebiet- und Abteilungsebene) den **verstärkten Einsatz von Personal Computern** (PC) festgestellt. Während in den Vorjahren in der Regel der Einzelplatz-PC anzutreffen war, werden jetzt mehr und mehr **vernetzte PC-Systeme** betrieben (Client-Server-Modell). Bei solchen DV-Systemen lassen sich Datenschutz- und Datensicherheitsprobleme leichter in den Griff bekommen, weil die angebotene Netzwerksbetriebs-Software häufig bereits wichtige Sicherheitskomponenten enthält. Beim Einsatz von Einzelplatz-PC fordere ich je nach Sensibilität des gespei-

cherten Datenmaterials die Implementierung zusätzlicher **Zugriffsschutz-Software,** die meist auch Verschlüsselungskomponenten enthält.

Besonders mustergültig sind die im Zusammenhang mit Neubauten verwirklichten Datensicherheitsmaßnahmen bei der KDZ Landshut der AKDB und bei der Landesversicherungsanstalt Unterfranken.

19.2.3 Forderungen an die polizeiliche Datenverarbeitung

In den letzten Jahren sind die Polizeidirektionen und -inspektionen mit sog. **Arbeitsplatzsystemen** ausgerüstet worden. Diese Arbeitsplatzcomputer (APC) eröffnen den Benutzern im Rahmen des Informationssystems der Bayerischen Polizei (IBP) auch einen Zugriff auf Dateien anderer Stellen (LKA, BKA, KBA usw.).

Meine technisch-organisatorischen Prüfungen im Polizeibereich konzentrierten sich auf die Überprüfung der **Datensicherheit** dieser Rechner. Dabei stellte sich heraus, daß aufgrund der **DV-systembedingten Mängel** noch einige Nachbesserungen bei den Maßnahmen zum Zugriffsschutz, zur Benutzerverwaltung und zur Beweissicherung notwendig sind.

Das Bayerische Staatsministerium des Innern wurde über die von mir festgestellten Datensicherheitsmängel informiert. Das Ministerium hat mir eine Überprüfung zugesagt.

19.2.4 Forderungen an Landratsämter

Die technisch-organisatorischen Datenschutzprüfungen von Landratsämtern in den vergangenen Jahren haben gezeigt, daß bei der Datenverarbeitung bestimmte **Sicherheitsmängel** immer wieder auftreten:

Zugriffsberechtigungen
Der Werdegang und die Vollzähligkeit der einzelnen Benutzerberechtigungen (auch für ausgeschiedene Mitarbeiter) sind häufig nicht revisionsfähig dokumentiert. Soweit überhaupt eine Dokumentation vorhanden ist, geht aus ihr zumeist nicht hervor, wer wann mit welcher Benutzerkennung und welchen Berechtigungen auf das DV-System zugreifen darf bzw. durfte.

Paßwortvergabe
Für die Paßwortvergabe werden den einzelnen Benutzern oftmals nur unzureichende Anweisungen vorgegeben. So werden beispielsweise immer noch **Trivialpaßwörter** und Zeichenfolgen, die sich aus mehreren gleichen Zeichen zusammensetzen, verwendet. Auch die Mindestlänge – es sollten 6 Zeichen sein – von Paßworten wird nicht eingehalten. Vielen Benutzern ist es – entgegen meinen wiederholten Forderungen – noch nicht möglich, ihr **Paßwort selbst zu vergeben** und zu ändern. Wenn das eingesetzte Betriebssystem eine solche Verfahrensweise nicht gestattet, sind **organisatorische** Maßnahmen zu ergreifen, welche die erforderliche Paßwortsicherheit gewährleisten. Gegebenenfalls ist zur Sicherstellung dieser Vorgaben eine entsprechende Zusatzsoftware einzusetzen.

Reaktionen des DV-Systems auf Fehlversuche
Der Einsatz einer **Zusatzsoftware** ist gelegentlich auch erforderlich, um Eindringversuchen rechtzeitig begegnen zu können. Dazu muß ein Anmeldedialog nach dreimaliger fehlerhafter Systemanmeldung abgebrochen und das entsprechende Endgerät „out of service" gesetzt werden. Den Ursachen für einen mißglückten Anmeldeversuch ist unbedingt nachzugehen.

Auswertung der Log-Dateien
Die von den Betriebssystemen bzw. DV-Verfahren erzeugten Protokolldateien werden zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung weder regelmäßig auf Unregelmäßigkeiten überprüft noch für spätere Revisionszwecke über einen längeren Zeitraum (ca. ein Jahr) aufbewahrt.

Einsatz von Arbeitsplatzcomputern (APC)
Bei manchen Landratsämtern wird die Hard- und Software nicht zentral beschafft, so daß ein Überblick über die eingesetzten Geräte, die installierte Software und die eingesetzten Verfahren fehlt. Die **Verpflichtung der Benutzer** zur Einhaltung vorgesehener und gebotener Datensicherheitsmaßnahmen, wobei die Benutzung nichtlizensierter Software zu verbieten ist, wird oftmals übersehen. Trotz wachsender Bedrohung durch **Computerviren** stellt der Einsatz geeigneter **Virenschutzprogramme** noch die Ausnahme dar.

Dokumentation
Manche Landratsämter entwickeln – hauptsächlich im PC-Bereich – eigene DV-Verfahren. Dabei wird jedoch häufig auf das Anlegen einer **aktuellen Programmdokumentation** verzichtet. Diese ist jedoch unbedingt erforderlich, damit sich bei einem Personalwechsel ein sachverständiger Nachfolger in einer angemessenen Zeit einarbeiten kann. Zu dokumentieren sind auch alle Programmänderungen. Für Programmaufträge und Programmänderungsanträge aus den Fachabteilungen der Landratsämter ist ein schriftliches, revisionsfähiges Auftragsverfahren einzuführen.

Datenträgeraufbewahrung
Sicherungsdatenträger (Streamer Tapes, Magnetbänder und Disketten) können mancherorts nicht zugriffs- und brandsicher aufbewahrt werden, da es an entsprechenden geeigneten Data Safes (S 120 DIS) mangelt.

Katastrophenvorsorge
Im Rahmen meiner Prüfungen habe ich den Landratsämtern stets empfohlen, zusammen mit den Hardware-Herstellern oder der AKDB ein Backup-Konzept für den Notfall zu erarbeiten, um im Ernstfall die Zeitdauer des Ausfalls der Datenverarbeitung möglichst kurz zu halten.

Entsorgung von Datenträgern
Einige Landratsämter nahmen irrtümlich an, daß ein Wartungsvertrag mit dem Hardware-Hersteller auch die datenschutzgerechte Wartung und Entsorgung der **Fest-**

platten für den Rechner gewährleiste. Für die Wartung und Entsorgung außer Haus müssen in einem solchen Wartungsvertrag jedoch **zusätzliche** vertragliche Regelungen getroffen werden, in denen die erforderlichen Sicherheitsmaßnahmen, wie Löschung vor der Wiederauslieferung, Geheimhaltungsverpflichtung, vorzugeben sind.

Für die Entsorgung von **Papierunterlagen** mit schutzwürdigen personenbezogenen Daten sind nicht immer leistungsfähige Aktenvernichter vorhanden. Ich empfehle den Landratsämtern, bei einer Papierentsorgung durch ein beauftragtes Unternehmen, gelegentlich auch die Zuverlässigkeit dieser Entsorgungsart vor Ort zu überprüfen.

Einbindung des Datenschutzbeauftragten
Die örtlichen Datenschutzbeauftragten werden nicht immer in die DV-Verfahrensabläufe, etwa bei der Zuteilung von Benutzerberechtigungen, eingebunden.

Erlaß von Richtlinien
Noch nicht alle Landratsämter haben Datenschutzrichtlinien für die ordnungsgemäße Benutzung der DV-Anlage, die datenschutzgerechte Entsorgung von Papierunterlagen oder – soweit noch vorhanden – die Führung von manuellen Karteien erstellt. Die Einhaltung dieser Vorschriften sollte durch den internen Datenschutzbeauftragten überwacht werden.

Aufbewahrung personenbezogener Unterlagen
Allen Landratsämtern empfehle ich, in Amtsbereichen, in denen besonders sensible personenbezogene Daten verarbeitet werden, zur Aufbewahrung dieser Unterlagen stabile abschließbare Behältnisse zu benutzen, damit Unbefugte in solche Unterlagen (Karteien, Akten) keinen Einblick erhalten können.

Den Bayerischen Landkreistag habe ich von diesen Mängeln unterrichtet und gebeten, den Landkreisen diese Beanstandungen und Empfehlungen zur Kenntnis zu geben, damit diese von sich aus ihre Datenverarbeitung daraufhin überprüfen und vorhandene Mängel beseitigen können.

19.2.5 Forderungen an Gemeinden

Bei der Kontrolle kommunaler Dienststellen habe ich häufig folgende Mängel an Datenschutz- und Datensicherheitsmaßnahmen festgestellt:

Benutzerrechte
Die Vergabe und Verwaltung von Benutzerrechten sind häufig nicht revisionsfähig. Wem wann welche Zugriffsberechtigungen erteilt worden sind, ist dann nicht nachvollziehbar. Gerade in den in der Regel überschaubaren Amtsbereichen von Gemeinden werden die Benutzerrechte „unbürokratisch" meistens ohne schriftliche Anforderung der Fachbehörde gleichsam „auf Zuruf" vergeben, weil man alle Mitarbeiter zu kennen glaubt. Es kommt vor, daß ausgeschiedenen oder erkennbar länger abwesenden Mitarbeitern, z.B. bei Inanspruchnahme von Mutterschutz- oder Kindererziehungszeiten, die Zugriffsberechtigungen erhalten bleiben. Es ist auch immer wieder festzustellen, daß Auszubildende, die sich für einige Monate auf Lehrgängen befinden oder ihre Ausbildungszeit abgeschlossen haben, in den Benutzertabellen weiterhin als zugriffsberechtigt erscheinen. Meine Forderung lautet deshalb, daß die Personalstelle den Benutzerverwalter über das Ausscheiden oder längere Abwesenheiten unterrichtet. Ferner ist die Vergabe von Benutzerrechten zu formalisieren, ihre Aktualität sicherzustellen und somit ihre Nachprüfbarkeit zu gewährleisten.

Autonome Datenverarbeitung
Immer mehr Gemeinden setzen, zumindest in Teilbereichen ihrer Verwaltung, autonome DV-Systeme zur Abwicklung ihrer Verwaltungsaufgaben ein. Dabei werden die Anforderungen an die Sicherheit solcher autonomer Einrichtungen nicht selten übersehen. So sichert man die aktuellen Daten nur gelegentlich, bewahrt die Sicherungsdatenträger ungesichert im Schreibtisch des Sachbearbeiters auf, übersieht, daß bestimmte Betriebssysteme (z.B. MS-DOS) für die Verarbeitung sensibler Informationen keinen Zugriffsschutz bieten, überläßt die Beschaffung von Hard- und Software den betreffenden Amtsbereichen selbst und verliert damit den Überblick über die installierten Verfahren. Oft treffen die Gemeinden auch keine Vorsorgemaßnahmen, um im Notfall Ausfallzeiten ihrer eigenen Datenverarbeitung durch geeignete Backup-Regelungen möglichst schnell zu überbrücken.

Ich weise daher in meinen Prüfberichten darauf hin, daß beim Umstieg von einer Auftragsdatenverarbeitung, etwa bei der AKDB, auf autonome Datenverarbeitung in Eigenregie für die speichernde Stelle Datensicherheitsmaßnahmen (z.B. Zutrittsschutz zum Rechnerraum, Außensicherung des Rechnerraums, Zugriffsschutz auf gespeicherte Daten, Datensicherung, gesicherte Aufbewahrung der Sicherungsdatenträger, Backup-Regelungen) erforderlich werden, die bisher in der Regel der Auftragnehmer erbracht hat.

Parteiverkehr
Die einzelnen Amtsbereiche einer Gemeindeverwaltung haben mehr oder weniger starken Parteiverkehr abzuwickeln. Schwerpunkte bilden die Einwohnermelde- und Paßämter. Gerade in Spitzenzeiten des Parteiverkehrs ist aber der Persönlichkeitsschutz des einzelnen Bürgers in diesen Behörden häufig nicht mehr gewährleistet. Es fehlen ausreichend große Wartezonen mit der Folge, daß sich die Wartenden bis an den Sachbearbeiterplatz drängen und die Gespräche ihres Vordermanns mit dem Sachbearbeiter mitverfolgen können. Bildschirme dürfen nicht so aufgestellt werden, daß Dritte den Bildschirminhalt mitlesen können. Aufrufsysteme oder abgeschottete Sachbearbeiterplätze sind selten anzutreffen. Hinweise auf die Möglichkeit einer vertraulichen Einzelfallbehandlung in einem gesonderten Dienstzimmer sind ebenfalls kaum zu finden.

Wenn ich auch nicht verkenne, daß oft bauliche Gegebenheiten einem zufriedenstellenden Persönlichkeitsschutz entgegenstehen und die Haushaltsmittel knapp sind, bitte ich die Gemeinden dennoch, alle ihnen zu Gebote stehenden Möglichkeiten auszuschöpfen, um den Persönlichkeitsschutz des einzelnen Bürgers weitestgehend zu gewährleisten.

19.3 Technische Einzelprobleme

19.3.1 Unix-Sicherheit

Über den Stand der Sicherheit beim Einsatz von Unix-Systemen habe ich im 14. Tätigkeitsbericht ausführlich berichtet, so daß an dieser Stelle lediglich noch einmal auf einige notwendige Sicherheitsmaßnahmen beim Betrieb dieser Rechner hinzuweisen ist:

- Jeder Benutzer muß über eine **eigene Benutzerkennung** und ein **individuelles Paßwort** verfügen. Gruppenkennungen sind zu verbieten.
- Die Dokumentation der Benutzerverwaltung hat **revisionsfähig** zu erfolgen.
- Die Einträge **ausgeschiedener Mitarbeiter** in der Benutzerkennungsdatei sind zur Vermeidung einer mißbräuchlichen Benutzung unverzüglich zu löschen.
- Die meisten Unix-Derivate bieten die Möglichkeit der **Paßwortselbstvergabe und -änderung** durch den Benutzer, wobei dieser auch zur Verwendung von Sonderzeichen oder numerischen Zeichen bei der Paßwortgestaltung gezwungen werden kann. Hiervon ist Gebrauch zu machen.
- Der regelmäßige **Paßwortwechsel** und eine Paßwortmindestlänge sollen maschinell erzwungen werden.
- Technisch nicht möglich ist in der Regel eine Zurückweisung von Trivialpaßworten anhand einer sogenannten Stopliste. Hier müssen organisatorische Maßnahmen greifen (Erlaß einer Dienstanweisung sowie die Schulung und Sensibilisierung aller Anwender).
- Herstellerseitig vorgegebene **Installationspaßworte** sind unverzüglich zu ändern bzw. nicht benötigte Kennungen zu löschen.
- Die **Zugriffsrechte** der Anwender sind auf das für sie erforderliche Minimum (z. B. ausschließlicher Zugriff auf die installierte Textverarbeitung) mit Hilfe eines Einstiegsmenues zu beschränken.
- Die **Betriebssystemebene** (Shell) ist für normale Benutzer zu sperren.
- Die LOGIN-Prozedur oder der Zugriff auf geschützte Daten kann **zeitlich beschränkt** werden (z. B. auf die allgemeine Arbeitszeit) durch ein über den Prozeß „CRON" zeitgesteuertes Verändern des „Runstate" oder einer zeitlichen Steuerung der Anwendung.
- Nach jedem erfolgreichen LOGIN sind Datum und Uhrzeit des **letzten LOGINs** automatisch anzuzeigen, damit der Anwender eine zwischenzeitliche, mißbräuchliche Benutzung seiner Kennung erkennen kann.
- Die maschinell geführten **Protokolldateien** sollten – soweit möglich – regelmäßig hinsichtlich der aufgetretenen Sicherheitsverletzungsversuche überprüft werden.

19.3.2 PC-Sicherheit

Der Einsatz sogenannter Arbeitsplatzcomputer (APC) im Bereich der öffentlichen Verwaltung – manchmal sogar als Ersatz für ausgediente Großrechner – nahm wiederum zu. Obwohl ich in früheren Tätigkeitsberichten bereits wiederholt auf die damit verbundenen Gefahren bei dieser Art von Informationsverarbeitung hingewiesen und Lösungsmöglichkeiten zur Einhaltung der gebotenen Datensicherheit aufgezeigt habe, waren bei den Kontrollen Mängel festzustellen. Ich möchte deshalb nochmals auf einige wichtige **Datensicherheitsmaßnahmen beim Betrieb dieser Rechnertypen** hinweisen.

Anforderungen an PC-Softwareschutz

Das Betriebssystem eines Stand-alone-PC bietet standardmäßig in der Regel keinen effektiven **Zugriffsschutz,** so daß jeder – auch der unberechtigte – Benutzer freien Zugriff zu allen Komponenten des Rechners hat. Der Einsatz einer **Zusatzsoftware,** um nichtpriviligierte Benutzer abzuweisen und berechtigte Anwender daran zu hindern, nicht gewollte Operationen durchzuführen, ist somit erforderlich. Zweckmäßig ist es, wenn dieses Produkt auch eine **Protokollierungs-** und **Verschlüsselungsmöglichkeit** für die Datenkommunikation innerhalb eines Netzes bietet.

Wesentliche Anforderungen an eine Software, die den **Zugriff** auf die Daten eines Personal Computers schützen und die **Revisionsfähigkeit** der Verarbeitung gewährleisten soll, sind:

- Unabhängigkeit von eingesetzter Hardware und Verträglichkeit mit vorhandener Software
- Zugriffssicherung durch
  - Identifikation des Anwenders mit Benutzerkennung und Paßwort
  - Verstecken, Schreibschützen, Verschlüsseln und Sperren von Dateien und Verzeichnissen
  - Sperren des PC nach drei aufeinander folgenden Fehlversuchen
  - Sperren des PC außerhalb der allgemeinen Arbeitszeit und in Arbeitspausen (Software-Verriegelung)
  - Sperren der Betriebssystemebene für den normalen Anwender
- Kontrollierter Einsatz bzw. Sperren von bestimmten Betriebssystembefehlen, wie Kopieren, Löschen, Formatieren, Zugriff auf Diskettenlaufwerke
- Gewährleistung der Programm- und Datenintegrität
- Lückenlose Menueführung des Bedieners (Bedienerfreundlichkeit durch Unterstützung sogenannter „Help"-Tasten)
- Kein nennenswerter Leistungsverlust (Performance) durch Einsatz der Zusatzsoftware
- Flexibilität durch
  - globalen Schutz des Rechners und der Anwendungen

  - individuelle Festlegung einzelner Schutzkomponenten für einzelne Anwender bzw. Ressourcen
- Sperren aller nichtbenötigten Laufwerke
- Führung eines Log-Buches (Protokolldateien) durch Schreiben signifikanter Ablaufdaten
- Unterstützung des Systemverantwortlichen bei der Auswertung der Ablaufdaten
- Dokumentation der Benutzerprofile
- Zuweisung der benötigten Ressourcen für die einzelnen Benutzer
- Physikalische Neuformatierung eines Bereiches von gelöschten Dateien (eine logische Löschung der Dateien genügt meistens nicht)
- Gewährleistung der Wirtschaftlichkeit hinsichtlich
  - der Anschaffungskosten
  - der Wartung und Pflege sowie
  - des Schulungsaufwands.

In diesem Zusammenhang möchte ich darauf hinweisen, daß das Bayer. Staatsministerium für Ernährung, Landwirtschaft und Forsten ein Software-Paket namens PWLAN entwickelt hat, das zusammen mit den Funktionen eines Netzwerk-Betriebssystems einen guten Zugangs- und Benutzerschutz bietet und auch die Revisionsfähigkeit der Datenverarbeitung unterstützt.
Dieses Programm wird vom Ministerium auf Anforderung kostenlos zur Verfügung gestellt.

Verpflichtungserklärung

Im 11. Tätigkeitsbericht habe ich darauf hingewiesen, daß jeder PC-Benutzer eine Verpflichtungserklärung zur Beachtung datenschutzrechtlicher Anforderungen vor der erstmaligen Benutzung eines Personal Computers abgeben sollte. Diese Erklärung – ein Muster kann bei meiner Geschäftsstelle angefordert werden – sollte auf folgende Punkte eingehen:

- Meldung der Hard- und Software zu den Übersichten (Hard- und Software-Kataster, künftiges Anlagenverzeichnis)
- Verbot des Einsatzes privater Hard- und Software
- Vorgabe, auf den vorhandenen Personal Computern nur vor- und freigegebene Software einzusetzen
- Verbot des Einsatzes von selbsterstellter Software, Public Domain Programmen, Shareware und Computerspielen
- Ausschließlicher Einsatz lizensierter Software
- Verbot des Zugangs für unbefugte Personen zum PC sowie Verbot des Zugriffs auf Programme und Daten
- Ausschließliche Nutzung des PC für dienstliche und vorgegebene Zwecke
- Verbot der Verfälschung oder Weitergabe von Programmen und Daten
- Meldung personenbezogener Dateien an den internen Datenschutzbeauftragten
- Einhaltung der vorgeschriebenen Datenschutz- und Datensicherheitsmaßnahmen
- Verpflichtung zur Duldung der Revision durch dazu berechtigte Personen
- Durchführung regelmäßiger Datensicherungen.

Virenbekämpfung

Die Anzahl unterschiedlicher Computerviren nahm auch im Jahre 1993 wieder erheblich zu: So dürften bis Ende des Jahres mehr als 2.500 verschiedenartige Viren bekannt sein. Infolge der stetig zunehmenden Vernetzung von Personal Computern und der damit verbundenen Möglichkeit der Ausweitung eines Virenbefalls **wächst die Gefahr für die Sicherheit von Rechnern und Rechnernetzen.** Moderne PC-Betriebssystem-Versionen (z. B. MS-DOS 6.0 und Novell DOS 7.0) enthalten deshalb bereits einen **Virenscanner** zur Überwachung des Computers gegen Virenbefall und Entfernung entdeckter Viren. Scanner bieten aber **keinen vollständigen Schutz** vor Virenbefall, da sie nur die Viren suchen und bekämpfen können, die ihnen bereits bekannt sind. Gute Virenscanner bieten nach allgemeinen Schätzungen im Zeitpunkt ihres Erscheinens die Sicherheit, bis zu 85 Prozent aller Viren erkennen zu können. Jede Behörde sollte daher darauf achten, daß nur Scanner von solchen Anbietern erworben werden, die einen regelmäßigen Update-Service anbieten. Ein Virenschutzprogramm sollte stets das Datum seiner letzten Aktualisierung anzeigen, damit der Anwender erkennt, wieviel Zeit seit dem letzten Update vergangen ist. Veraltete Virensuchprogramme sollten den Benutzer vor ihrem eigenen Verfallsdatum warnen, damit sich dieser rechtzeitig um ein neues Update kümmern kann.

Mittlerweile kommt eine **Welle neuer Viren** auf die Personal Computer zu, die mit den bisherigen Mitteln **weder entdeckt noch bekämpft** werden können. Es handelt sich um Viren, die sich nach einer erfolgten Infektion eines Rechners verändern und eine nicht wiedererkennbare Gestalt annehmen; sie codieren sich. Gegen diese neue Generation der Viren vermögen auch gute Anti-Viren-Programme nichts auszurichten. Besondere Gefahr droht auch durch die Tatsache, daß sich DV-Laien mittels eines auf dem Markt erhältlichen Viren-Generators, wie „Dark Avanger Mutation Engine", Viren selbst erzeugen können. Dagegen scheinen nur noch hardwarebasierende Konzepte, wie „Thunderbyte" von Data-5, Schutz zu bieten. Bei Thunderbyte handelt es sich um eine PC-Einsteckkarte, die bereits mit Beginn des Boot-Vorgangs das System auf verdächtige Aktionen überwacht, diese dem Benutzer meldet und – falls gewünscht – abblockt.

19.3.3 Sicherheitsmaßnahmen beim Einsatz des Telefax-Dienstes

Im 12. Tätigkeitsbericht wurde bereits über Sicherheitsmaßnahmen bei der Nutzung des Telefax-Dienstes der Telekom berichtet. In der Zwischenzeit hat sich die Zahl der Telefax-Teilnehmer stark erhöht und mit ihr auch die Fluktuation der Fax-Anschlüsse, so daß die Anzahl der Irrläufer beim Telefax-Dienst der Telekom ständig zugenommen haben soll. Als Grund hierfür wird häufig angegeben, daß, wenn ein Kunde, etwa wegen Umzugs, seinen Fax-Anschluß kündigt, die Telekom seine Telefax-Nummer sofort an einen anderen, neu hinzugekommenen

Teilnehmer weitergibt. Die Telekom hat es bisher abgelehnt, eine freiwerdende Fax-Nummer erst nach einer bestimmten Frist wieder zu verwenden.

Um dem Risiko des Fehlversands zu begegnen, sollte sich der Absender im Zweifelsfalle vor dem Versand durch einen Anruf vergewissern, ob er mit der Fax-Nummer auch den gewünschten Adressaten erreicht. Beim Telefax-Versand zwischen Behörden dürfte ein Wechsel der Fax-Nummer allerdings sehr selten auftreten.

Es gibt Behörden, die sogar ganz auf den Telefax-Dienst verzichten, wenn nicht in jedem Fall sichergestellt ist, daß das übertragene Dokument den Adressaten direkt erreicht oder Gefahr besteht, daß der Inhalt des Dokuments Personen zugänglich wird, für die dieses nicht bestimmt ist. Schließlich sollte der Grundsatz befolgt werden, was am Telefon nicht gesagt werden darf, darf wegen der Abhörmöglichkeiten auf dem Transportweg auch nicht gefaxt werden.

Zur ordnungsgemäßen Abwicklung des Telefax-Dienstes empfiehlt es sich außerdem, noch folgende organisatorischen Maßnahmen einzuhalten:

- Verwendung eines Vorblatts, aus dem Absender und Empfänger sowie die Anzahl der übertragenen Seiten ersichtlich sind
- Aufbewahrung des Übertragungsprotokolls für Beweissicherungszwecke
- Sichere Unterbringung des Telefax-Gerätes, damit Unbefugte keine ankommenden Schriftstücke entnehmen und vom Inhalt abgehender Dokumente nicht Kenntnis erhalten können
- Verwendung von Sicherheits-Telefax-Geräten, die angekommene Dokumente erst nach Eingabe eines Paßworts ausdrucken
- Bei Rückgabe geleaster Geräte ist zu kontrollieren, ob alle Speicher (Telefaxe, Sendeprotokolle, Kurzwahlnummern) gelöscht wurden, damit keine Daten an den nächsten Benutzer gelangen können.

19.3.4 Katastrophenarchiv

Für die Aufbewahrung der Sicherungen von Datenbeständen und Programmen sind umfangreiche Maßnahmen zu ergreifen. Neben einem **Datenträgerarchiv** bzw. Data Safe im Bereich des Rechenzentrums – um die täglich benötigten Datenträger möglichst griffbereit zu haben – ist ein vom Gebäude des Rechnerraums räumlich getrenntes **Katastrophenarchiv** einzurichten, in das regelmäßig Sicherungskopien aller relevanten Datenbestände ausgelagert werden, um nach einem Katastrophenfall (z. B. Brand im Rechnerraum) jederzeit auf die gesicherten Daten und Programme zugreifen zu können. Auch dieses Katastrophenarchiv sollte einen verläßlichen Schutz gegen Beschädigung, Zerstörung, Diebstahl, Mißbrauch und Verlust der Datenträger bieten, indem es – soweit möglich – gegen Feuer, Brandgase, Wasser, Explosion und andere äußere Einflüsse gesichert ist und überdies einer verschärften Zugangskontrolle unterliegt. Neben der Aufbewahrung der Sicherungsdatenträger in einem Data Safe eines anderen Gebäudes oder in einer Außen- oder Zweigstelle der Behörde bietet sich hierbei die Auslagerung aktueller Sicherungsbestände in einem Bankschließfach an.

19.3.5 Persönlichkeitsschutz im Sozialbereich und Maßnahmen zum Schutz der dort Beschäftigten

Das Sozialamt einer kreisfreien Stadt hat mich um Prüfung gebeten, ob und inwieweit sich das **zunehmende Sicherheitsbedürfnis** der Bediensteten auf den technisch-organisatorischen Datenschutz auswirkt.

Unter Hinweis auf das informationelle Selbstbestimmungsrecht der Bürger hatte ich zunächst die Meinung vertreten, daß die Dienstzimmer des Sozialamts nach Möglichkeit nur mit einem Sachbearbeiter besetzt sein sollten. Bei dieser Bewertung war bisher die **Sicherheit der Bediensteten** kein dringliches Thema. Wegen aktueller Vorfälle muß jedoch künftig beim technisch-organisatorischen Datenschutz die **Fürsorgepflicht des Dienstherrn** gegenüber den Mitarbeitern stärker berücksichtigt werden, da sich inzwischen Bedienstete von Sozialämtern häufig weigern, aus Angst vor massiven Bedrohungen durch Antragsteller und Petenten Einzelzimmer zu beziehen. Auch der Datenschutz hat diese Entwicklungen künftig zu beachten.

Bei Unterbringung von Sozialamtsbediensteten in Einzelzimmern habe ich unter Berücksichtigung des Persönlichkeitsschutzes der Petenten und zum Schutz der Mitarbeiter folgende Maßnahmen vorgeschlagen:

- Offenlassen der Zimmerverbindungstüren während des Parteiverkehrs, damit eine Rufverbindung mit anderen Bediensteten besteht
- Abtrennung des Besucher- vom Arbeitsbereich durch Einbau eines von Wand zu Wand reichenden Tresen
- Einbau von Alarmeinrichtungen, mit denen ein bedrohter Sachbearbeiter Hilfe durch seine Kollegen herbeiholen kann.

Trotz dieser neuen Situation sollten die betroffenen Dienststellen den Persönlichkeitsschutz der Bürger nicht mehr als unbedingt erforderlich einschränken.

19.3.6 Datenhaltung auf maschinenlesbaren Datenträgern als Ersatz für die Aufbewahrung von Originalakten

Mitunter wird an mich die Frage herangetragen, welche Sicherheitsmaßnahmen bei der Umsetzung von Akten auf einen anderen Datenträger zu beachten sind. Bei der Datenübertragung von Originalakten auf elektronische Datenträger oder auf Mikrofilm hat man zwischen folgenden Fällen zu unterscheiden:

■ **Übertragung der Originalakten auf Mikrofilm oder -fiche**

Der Mikrofilm oder Mikrofiche gilt heute als beliebtes Archivierungsmedium. In der Buchführung werden seit

langem Unterlagen, die sich auf dem Medium Mikrofilm befinden, als zulässig anerkannt. Die Ordnungmäßigkeit der mikroverfilmten Unterlagen ist allerdings durch ein Verfilmungsprotokoll zu belegen, aus dem hervorgeht, wer die Originale zu welcher Zeit verfilmt hat. An verfilmten Unterlagen sind keine Änderungen möglich. Manipulationen müßten somit vor der Verfilmung vorgenommen worden sein.

■ **Übertragung der Originalakten auf optischen Datenträger**

Analog ist auch hier ein Protokoll zu fordern, aus dem die rechtmäßige Übertragung der Unterlagen hervorgeht. Da die optische Platte nur einmal beschrieben werden kann, also ein WORM-Speicher (write once read many) ist, können Manipulationen an gespeicherten Dokumenten ausgeschlossen werden. Die gespeicherten Dokumente können auf einem Bildschirm angezeigt und über einen Drucker ausgedruckt werden. Da die Information nicht in digitaler Form, sondern als sog. „non-coded information" vorliegt, sind gezielte Verfälschungen bei der Anzeige und beim Ausdrucken ebenfalls nicht möglich.

■ **Übertragung der Dokumente in digitale Form**

Zur Zeit sind nur wenige Verfahren bekannt, bei denen Dokumente so in digitale Form umgewandelt werden können, daß sich die Inhalte mit Datenverarbeitungsprogrammen weiterverarbeiten lassen. Die Verfahren der Schriftenerkennung sind heute noch zu wenig ausgereift, als daß unterschiedliche Schriftarten oder gar Handschriften erkannt werden könnten. Schließlich können Dokumente auch durch Computerverfahren (Textverarbeitung) und manuelle Eingaben am Bildschirm entstehen.
Hier sind digitale Speicherungen jederzeit in der Form änderbar, daß im Nachhinein nicht erkennbar ist, ob ein Dokument geändert wurde oder nicht, sofern im System nicht vermerkt wurde, wann ein Dokument erstellt sowie, ob und wann es geändert wurde. Hier ist also auf die **Revisionsfähigkeit** aller Aktionen zu achten.

Grundsätzlich empfiehlt es sich, **wichtige Dokumente im Original** aufzubewahren, um dieses im Bedarfsfalle als Beweis für die Echtheit heranziehen zu können. Das wird seit langem bei der Mikroverfilmung von Altakten so gehandhabt. Auf Mikrofilm oder auf elektronischen Datenträgern gespeicherte Dokumente sind jederzeit auf den Datenträger Papier zu bringen. Für Revisionszwecke muß das Protokoll über die Erstellung elektronischer Dokumente neben dem Zeitstempel (Datum und Uhrzeit der Erstellung) vor allem den Erfasser oder Ersteller enthalten.

Aus der Sicht des Datenschutzes dürften diese Beweismittel ausreichen, da für Zwecke der Beweissicherung auch in anderen Fällen elektronische Protokolle Stand der Technik sind und anerkannt werden.

20. Datenschutzregister

Durch das Bayerische Datenschutzgesetz vom 23. Juli 1993 ist die **Verordnung** über das Datenschutzregister vom 23. November 1978 und Art. 7 des Bayerischen Datenschutzgesetzes vom 28. April 1978 mit Wirkung vom 1. August 1993 **außer Kraft** getreten: Vom 1. August 1993 an waren **keine Registermeldungen** mehr erforderlich. Von dieser Regelung ausgenommen bleiben aber **Sozialbehörden,** die unter die Regelungen des § 79 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) fallen. Abgesehen vom **geringen Informationswert** für die Bürger sprechen auch Gründe der **Verwaltungsvereinfachung** für den Wegfall des zentralen Registers beim Landesbeauftragten für den Datenschutz.

In der Zeit vom 24. Oktober 1992, dem Zeitpunkt der letzten Veröffentlichung eines Nachtrages zur Übersicht zum Datenschutzregister, bis zum Außerkrafttreten der bisherigen Regelungen am 31. Juli 1993 hat sich der Umfang des Datenschutzregister um weitere 1.100 Dateien auf insgesamt **24.800 Dateien** erhöht.

Die Zahl der Bürger, die jährlich nachfragen, bei welchen Behörden Daten über sie gespeichert sein können, ist im Berichtszeitraum auf niedrigem Niveau gleich geblieben.

Nach Art. 27 des neuen BayDSG muß die speichernde Stelle ab 1. März 1995 ein sog. **Anlagen- und Verfahrensverzeichnis** führen, das behördenbezogen die Rolle des Datenschutzregisters übernehmen kann, wenn sich ein Petent an diese Stelle wendet und Auskunft über gespeicherte Daten wünscht.

21. Datenschutz beim Bayerischen Rundfunk

Durch § 1 Nr. 15 des Gesetzes zur Änderung des Bayer. Rundfunkgesetzes vom 23. Juli 1993 (BayRS 2251-1-K) wurden mit Wirkung vom 1. August 1993 bereichspezifische Datenschutzvorschriften in das Bayer. Rundfunkgesetz (BayRG) eingearbeitet. Nunmehr wird nach Art. 19 d BayRG die Einhaltung des Datenschutzes im Bayer. Rundfunk vom dortigen Beauftragten für den Datenschutz überwacht, der in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist.

Zum gleichen Zeitpunkt wurde Art. 21 des Bayer. Datenschutzgesetzes außer Kraft gesetzt. Nach dieser Bestimmung hatte der Datenschutzbeauftragte des Bayer. Rundfunks bislang seinen Tätigkeitsbericht auch dem Landesbeauftragten für den Datenschutz zu übermitteln (Art. 21 Abs. 3 Satz 6 BayDSG). Aus dieser Bestimmung hatte ich bisher die Aufgabe für mich abgeleitet, über den Datenschutz beim Bayerischen Rundfunk zu berichten. Im Hinblick auf die neue Rechtslage sehe ich nunmehr davon ab.

22. Der Beirat

Die Mitglieder des Beirates werden nach Art. 29 Abs. 2 des alten BayDSG für vier Jahre, die Mitglieder des Landtags für die Wahldauer des Landtags bestellt. Im Berichtszeitraum gehörten dem Beirat an:

Ordentliche Mitglieder	**Vertreter**
die Landtagsabgeordneten	
Franz Brosch	Dr. Hans Gerh. Stockinger
Alois Braun	Dr. Helmut Müller
Franz Meyer	Wilhelm Wenning
Markus Sackmann	Georg Grabner
Dr. Klaus Hahnzog	Armin Nentwig
Carmen König	Joachim Wahnschaffe
die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
für die Staatsregierung	
Christian P. Wilde Ministerialrat im Bayer. Staatsministerium des Innern	Hubert Kranz Ministerialrat im Bayer. Staatsministerium der Finanzen
für die Sozialversicherungsträger	
Dr. Ludwig Bergner Erster Direktor der Landesversicherungs- anstalt Oberbayern	Herbert Schmaus, bis 15.6.93 Gerhard Wunderlich, ab 15.6.93 Direktor, Geschäftsführer des BKK Landesverbands Bayern
für die Kommunalen Spitzenverbände	
Klaus Eichhorn Geschäftsführender Direktor der Anstalt für Kommunale Datenverar- beitung in Bayern	Hanns Herrlitz Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern
für den Verband der Freien Berufe in Bayern e.V.	
Erwin Stein, MdL Präsident der Steuer- beraterkammer München	Winfried Wachter Präsidiumsmitglied des Verbandes der Freien Berufe in Bayern e.V.

Den Vorsitz im Beirat führt Franz Brosch, MdL; Stellvertreterin ist Carmen König, MdL.

Der Beirat befaßte sich in seinen Sitzungen am 02.03.1993, 09.03.1993, 20.04.1993, 22.06.1993 und 05.10.1993 insbesondere mit folgenden Themen:

- Beratung des 15. Tätigkeitsberichtes
- Berichte über Prüfungen und Beanstandungen
- Berichte von Arbeitskreisen und Datenschutzkonferenzen
- Novellierung des Bayerischen Datenschutzgesetzes
- Entwürfe zu einem Bayerischen Petitionsgesetz bzw. Eingabegesetz
- Kontrollen in der Landwirtschaft aufgrund der EG-Verordnung zur Einführung eines integrierten Verwaltungs- und Kontrollsystems für bestimmte gemeinschaftliche Beihilferegelungen
- Zugriff des Staatsministeriums für Ernährung, Landwirtschaft und Forsten auf die Daten der Ämter für Landwirtschaft
- Bekanntgabe persönlicher Daten einer Partei an die Gegenpartei und an die Öffentlichkeit im Rahmen von Gerichtsverfahren
- inhaltlicher Umfang von Einstellungsbescheiden nach der Strafprozeßordnung
- Datenabgleich zur Feststellung von Sozialleistungsmißbrauch sowie Novellierung des Sozialgesetzbuches
- Entwurf einer EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

23. Vorträge und Seminare über Datenschutz

Die Nachfrage nach Referenten für Vorträge zum Datenschutz und zur Datensicherheit hielt unvermindert an. Soweit die Arbeitsbelastung durch vorrangige Datenschutzkontrollen die Übernahme von Vorträgen und Seminaren zuließ, habe ich den Anfragen entsprochen.

Beim **Landesamt für Statistik und Datenverarbeitung** und bei der **Bayerischen Verwaltungsschule** waren mehrere Vorträge und Seminare zu halten. Neben einer allgemeinen Einführung in Datenschutz und Datensicherheit befaßten sich die Veranstaltungen mit speziellen Themen wie „Datenschutz in der Kriegsopferfürsorge", „Datenschutz im Sozialamt". An der Fort- und Ausbildung der Bayer. Polizei wirkten meine Mitarbeiter mit mehreren Vorträgen mit.

Neben diesen regelmäßig laufenden Fortbildungsmaßnahmen waren **Vorträge** zu halten vor Personalräten, Schulräten eines Regierungsbezirkes, Mitarbeitern von Museen, Archiven und Bibliotheken, in Zusammenarbeit mit dem Staatsministerium der Justiz vor Gerichtsvollziehern, vor Sozialarbeitern aus dem Bereich der Altenhilfe, in der Akademie für Arbeitsmedizin über den Datenschutz im Gesundheitsbereich, in einer städtischen Akademie über den Schutz von Sozialdaten, im Fachhochschulbereich sowie vor einer Volkshochschule.

In den **neuen Ländern** besteht ein großer Ausbildungsbedarf für Fragen des Datenschutzes und der Datensicherheit. Meine Mitarbeiter haben in Sachsen und Thüringen in mehreren ein- oder zweitägigen Seminaren entsprechende Grundkenntnisse unter Berücksichtigung des jeweiligen Landesrechtes vermittelt. Dabei war von Vorteil, daß ein Mitarbeiter für die Dauer von 2 Jahren zum Aufbau des Datenschutzes nach Thüringen abgeordnet war und damit Erfahrungen über die Datenverarbeitung durch frühere Einrichtungen der DDR sammeln konnte.

24. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Datenschutzbeauftragten des Bundes und der Länder trafen sich 1993 zu zwei regulären Konferenzen.

1. **Schwerpunkte der Erörterungen waren**
   - Entwurf eines Umweltinformationsgesetzes des Bundes zur Umsetzung der EG-Datenschutzrichtlinie

- Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz
- Datei „Gewalttäter-Sport"
- Einsatz von elektronischen Observierungsmitteln in Wohnungen („Lauschangriff") zur Strafverfolgung und Grundrecht auf Datenschutz
- Erfolgskontrolle polizeilicher Befugnisse bei steigender Kriminalität
- Regelmäßige Datenübermittlung an die Rundfunkanstalten
- Abbau des Sozialdatenschutzes zur Aufdeckung des Mißbrauchs von Sozialleistungen
- Anwendung des Bundesdatenschutzgesetzes oder der Landesdatenschutzgesetze auf Unternehmen des privaten Rechts mit öffentlichen Aufgaben
- Datenschutz bei der Mobilkommunikation, im Mobilfunk (BOS-Funkverkehr), bei der Privatisierung der DBP-Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste
- Persönlichkeitsschutz und Medienprivileg
- Rechtliche Einordnung von Wartung und Fernwartung
- Elektronische Zahlungssysteme (automatische Autobahngebührenerfassung und kartengestützte Zahlungssysteme im öffentlichen Nahverkehr)
- Technische Möglichkeiten zur Durchführung und technische Maßnahmen zur Verhinderung des „Großen Lauschangriffs"
- Integriertes Verwaltungs- und Kontrollsystem (InVeKos) der EU-Mitgliedsstaaten im Bereich der Landwirtschaftsförderung
- Geschäftsordnung der Konferenz der Datenschutzbeauftragten.

2. **Einsatz von elektronischen Observierungsmitteln in Wohnungen („Großer Lauschangriff")**

   In der Konferenz am 26./27. Oktober 1993 in Berlin zeigte sich, daß hinter der vor einem Jahr in Stuttgart gefaßten „Entschließung" allenfalls noch eine knappe Mehrheit der Datenschutzbeauftragten steht. Auch unter den Datenschutzbeauftragten gewinnt die Einsicht an Boden, daß angesichts der Gefährlichkeit der Organisierten Kriminalität die bisherige Ablehnung dieses Fahndungsmittels nicht länger durchzustehen ist. Angesichts dieser gewandelten Einstellung der Teilnehmer sah der Vorsitzende von der Abstimmung über eine erneute Entschließung ab. Die anschließende Pressemitteilung über die angeblich weitere Ablehnung des „Großen Lauschangriffs" entsprach daher nicht der Auffassung der Datenschutzkonferenz.

3. **Abbau des Sozialdatenschutzes zur Aufdeckung des Mißbrauchs von Sozialleistungen**

   In der Konferenz gescheitert ist ein Vorstoß eines Landesbeauftragten, die angesichts des verbreiteten Mißbrauchs von Sozialleistungen verstärkten Mißbrauchskontrollen der Sozialhilfebehörden, Arbeitsämter, Krankenkassen und Rentenversicherer als „soziale Rasterfahndung" zu diskreditieren und den automatisierten Datenabgleich zwischen Sozialbehörden zur Aufdeckung von Sozialbetrug zu stoppen.

   Nach meiner Auffassung muß angesichts leerer Staatskassen, horrender Staatsverschuldung und des eisernen Zwangs zum Sparen der weit verbreitete Mißbrauch von Sozialleistungen durch dichtere Kontrollen der Angaben der Leistungsbezieher genauso eingeschränkt werden wie die Steuerhinterziehung. Bei dem Ruf nach möglichst perfektem Datenschutz wird häufig übersehen, daß auch Leistungsgerechtigkeit zu den Grundwerten unserer Verfassung gehört und der Staat nach dem **Zinsurteil** des Bundesverfassungsgerichts von 1991 aus dem **Gleichheitsgrundsatz** und dem **Willkürverbot** heraus sogar verpflichtet ist, **für ausreichende Kontrolle** zu sorgen, um die Ehrlichkeit der Steuerzahler und Sozialleistungsbezieher zu stützen.

4. **Geschäftsordnung der Konferenz der Datenschutzbeauftragten**

   In der Konferenz mahnte ich erneut die Vereinbarung einer Geschäftsordnung an, wie sie beispielsweise für die Ministerpräsidenten-Konferenz erlassen wurde. In der Geschäftsordnung muß insbesondere geregelt werden, unter welchen Voraussetzungen (Einstimmigkeits- oder Mehrheitsprinzip) Entschließungen der Konferenz zustande kommen.

Anlage 1: Beschluß der DSB-Konferenz vom 16./17. Februar 1993 zum Entwurf einer EG-Datenschutzrichtlinie

1. Die EG-Richtlinie darf das nationale Datenschutzrecht nur insoweit harmonisieren und nivellieren, als es sich als **Handelshemmnis im grenzüberschreitenden Verkehr** auswirkt. Ein über den harmonisierten EG-Standard hinausgehender Datenschutz im einzelstaatlichen Recht für Datenverarbeitung ohne grenzüberschreitenden Bezug muß nach dem Grundsatz der Subsidiarität zulässig bleiben.
2. Dem nationalen Gesetzgeber muß bei der Ausgestaltung der Methoden, wie er die Einhaltung des Datenschutzes gewährleisten und kontrollieren will, nach dem Grundsatz der Subsidiarität mehr Spielraum eingeräumt werden. Insbesondere muß ihm die Richtlinie gestatten, **die Meldepflicht zum Dateienregister,** vor allem im nichtöffentlichen Bereich, auf für den Datenschutz wirklich bedeutsame Dateien zu beschränken.

3. Die im Richtlinienentwurf vorgesehene **Unabhängigkeit der nationalen Datenschutzkontrollbehörden gegenüber Regierung und Exekutive** darf nicht aufgeweicht werden durch Bestimmungen, die es dem deutschen Gesetzgeber gestatten, die Institution der unabhängigen Datenschutzbeauftragten des Bundes und der Länder einzuschränken.

4. In der Richtlinie sollte dem einzelstaatlichen Gesetzgeber ausdrücklich die Option eröffnet werden, eine Kontrollinstitution innerhalb datenverarbeitender Stellen (**betrieblicher bzw. behördlicher Beauftragter** für den Datenschutz) vorzusehen.

Anlage 2: Entschließung zu kartengestützten Zahlungssystemen im Öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z.B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im Öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im Öffentlichen Nahverkehr können – wie skandinavische und auch deutsche Projekte aufzeigen – Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die „datenfreie Fahrt" zu ermöglichen. Im Öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld. Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.