Der Bayerische Landesbeauftragte

für den Datenschutz

19. Tätigkeitsbericht, 2000

Stand: 14.12.2000

1 Überblick

1.1 Datenschutzentwicklungen

1.1.1 Big Brother – Ende des Datenschutzes?

Angesichts der Sendung Big Brother, deren zweite Staffel derzeit mit einigem Erfolg läuft, stellen viele die Frage, ob in einer solchen Zeit Datenschutz überhaupt noch eine Berechtigung und eine Chance habe.

Diese Frage ist verständlich, wenn man berücksichtigt, dass das Erfolgsprinzip der Sendung gerade das Rund-um-beobachtet-werden einer Personengruppe ist. Das Erfolgsprinzip setzt gerade voraus, dass sich dieser Beobachtung niemand zu irgend einem Zeitpunkt entziehen kann. Glücklicherweise ist dieses „Erfolgsprinzip“ noch nicht zu 100% realisiert, es bestehen für mich aber keine Zweifel, dass die Sehquote umso höher sein wird, je umfassender die Beobachtungsmöglichkeiten sind, und zwar auch und gerade in den engsten Kreis der Privatsphäre, in den Intimbereich. Grenzen werden hier letztlich nur durch die staatliche Medienaufsicht gesetzt werden können.

Es ist hier nicht der Platz, allgemein über die Voraussetzungen und Auswirkungen einer solchen Entwicklung zu philosophieren. Aus der Sicht des Datenschutzes ist jedoch folgende Feststellung angebracht: Datenschutz ist wesentlich die informierte Selbstbestimmung über die Frage, wer, wann, was über einen weiß und was er mit diesem Wissen anfängt, oder, anders gesagt, die wesentlichen Datenschutzprinzipien sind Transparenz der Datenerhebung und Verwendung, Freiwilligkeit der Entscheidung und Zweckbindung der Datenverarbeitung.

Die Frage heißt also, haben diese Prinzipien angesichts der genannten Entwicklung noch ihre Berechtigung. Die Frage ist uneingeschränkt mit ja zu beantworten.

Entscheidend ist für mich, dass alle Teilnehmer an der Veranstaltung in voller Kenntnis dessen handeln, was auf sie zu kommt. Anders gesagt, die Datenerhebung ist transparent.

Sie ist auch freiwillig. Wesentliches Kriterium der Freiwilligkeit ist, dass der Willensentschluss

frei ist von physischem oder psychischem Zwang oder auch nur Druck, sei es objektiv oder auch nur subjektiv als solcher empfunden. Entscheidend ist zusätzlich, dass der Betroffene eine realistische Handlungsalternative hat. An manchen so genannten „freiwilligen Zustimmungserklärungen“ kann man ernsthafte Zweifel haben, legt man diese Kriterien an. So bin ich nicht der Auffassung, dass man wirklich von echter Freiwilligkeit der Zustimmung eines Vollzugsinsassen zu einer DNA-Analyse ausgehen kann. Auch scheinen mir Zweifel berechtigt, ob ein Betroffener, vor dem ein Polizist mit einem entsprechenden Zustimmungsformular steht, wirklich freiwillig im selbstbestimmten Sinn handelt. Auch hätte ich ernsthafte Zweifel an der Freiwilligkeit von Zustimmungen zu Datenverarbeitungen im Rahmen von medizinischen Behandlungsverträgen, wenn alle medizinische Leistungsträger die gleichen „Zustimmungen“ einholen, so dass der Betroffene keine Alternativen hat.

Die Entscheidung eines Betroffenen, bei Sendungen dieser Art mitzumachen, ist jedoch freiwillig ohne irgendeinen physischen oder psychischen Zwang. Das Sendeprinzip steht also auch mit dem Freiwilligkeitsprinzip nicht in Widerspruch.

Auch das Zweckbindungsprinzip wird durch die Veranstaltung nicht widerlegt, solange die „einzige“ Datenverarbeitung diejenige ist, dass alle Welt beobachten kann, was in dem Container zu jeder Minute geschieht, und dass alle Welt auf die Entwicklung in dem Container auf der Grundlage dieser Informationen Einfluss nehmen kann. Genau dieses ist der Zweck der Veranstaltung, jedermann weiß dies, jeder, der daran teilnimmt, akzeptiert das.

Aus der Existenz einer solchen Sendung kann auf einen allgemeinen Verzicht auf die Grundprinzipien des Rechts auf informationelle Selbstbestimmung nicht geschlossen werden.

Den Menschen ist es eben nicht gleich, welche Datenspuren durch ihre Arbeit mit dem Internet entstehen und wofür sie verwendet werden. Die Menschen nehmen es nicht gleichgültig hin, wenn sie ohne ihr Wissen in polizeilichen Dateien gespeichert werden und ihnen dieses bei einer Bewerbung in einem sicherheitsrelevanten Bereich entgegengehalten wird, oder sie bei einer Verkehrskontrolle oder bei der „Schleierfahndung“ mit der Begründung genauer unter die Lupe genommen werden, „dass über sie ja schon einiges vorliege“. Ich glaube auch nicht, dass es den meisten Menschen gleichgültig wäre, im öffentlichen Raum rund um die Uhr und auf jedem

Schritt von Videokameras verfolgt zu werden und jeden Schritt zur allfälligen Auswertung aufgezeichnet zu sehen. Die Menschen lässt es auch nicht unberührt, wenn ihre medizinischen Daten plötzlich auf der Internetseite eines Krankenhauses aller Welt zur Einsichtnahme offen stehen. Auch derjenige, dem der Satz „Von mir kann jeder alles wissen“ leicht über die Lippen geht, wird mit solchen „Datenverarbeitungen“ nicht einverstanden sein.
Datenschutz, das heißt der Schutz des Rechtes auf informationelle Selbstbestimmung, hat von seiner Berechtigung also nichts verloren.

Im Gegenteil: Angesichts der immer schneller wachsenden Möglichkeiten der Datenerhebung und -verarbeitung, angesichts der immer vielfältigeren Wünsche von - allgemein gesprochen - Datenverarbeitungsbedarfsträgern nach Nutzung der technischen Möglichkeiten, angesichts der zunehmenden Tendenz zu immer weiträumigeren Vernetzungen bin ich überzeugt, dass diesen immer größeren Möglichkeiten ein immer besserer Schutz des Bürgers vor unberechtigten Eingriffen in sein Recht auf informationelle Selbstbestimmung und damit letztlich in seine Freiheit als selbstbestimmter Bürger zur Seite stehen muss.

Zur Antwort auf die Frage, inwiefern dieses Postulat erfüllt ist, wo Defizite sind und welche Möglichkeiten zur Verbesserung ich sehe, soll dieser Bericht beitragen.

1.1.2 Neue Herausforderungen

Der Ruf nach der **Videoüberwachung** öffentlicher Räume hat sich verstärkt. Rechtsextreme Gewalttaten bisher nicht vorstellbaren Ausmaßes, ein heimtückisches Verbrechen mit tödlichen Folgen auf einem dunklen Parkplatz im Außenbereich der Münchner S-Bahn, Vergewaltigungen in S-Bahnen lassen den Ruf nach verstärkter Präsenz der Polizei in Form der Beobachtung von gefährdeten Plätzen verständlich erscheinen. Ich habe deshalb die Videobeobachtung in Einzelfällen nicht grundsätzlich abgelehnt.

Auf der anderen Seite muss einer Entwicklung entgegengetreten werden, die letztlich zu einer flächendeckenden Überwachungsinfrastruktur führen kann, in der jeder Bürger dauernd damit rechnen muss, beobachtet zu werden, und bei der er nicht weiß, wann, für wie lange und zu wel-

chen Zwecken aufgezeichnet wird.
Ich habe deshalb ein Gesetz gefordert, in dem die Voraussetzungen der Beobachtung öffentlicher Räume durch die Polizei, sowie die Einzelheiten der weiteren Datenverarbeitung geregelt werden. Das Gleiche gilt für Videobeobachtung durch andere öffentliche Bedarfsträger, wie z.B. Gemeinden, für die in Einzelfällen (z.B.Wertstoffhöfe) ebenfalls ein legitimes Interesse bestehen mag. Der Bayerische Landtag hat bei Gelegenheit der Beratung des Bayerischen Datenschutzgesetzes diese Frage andiskutiert. Der Vorsitzende der Datenschutzkommission erwartet eine Regelung noch in dieser Legislaturperiode. Im Einzelnen verweise ich auf Nrn. 5.6.4 und 8.8 dieses Berichts.

Neue Kommunikationsangebote der Verwaltung (Stichwort **e-government, elektronische Rathäuser**) können für die Bürgerinnen und Bürger wesentliche Erleichterungen bringen. Sie sollen zu Hause auf dem PC Informationen abrufen, sich Formulare herunterladen und endlich auch ganze Behördengänge auf diese Weise erledigen können. Die virtuelle Verwaltung wird und muss auch die Arbeitsabläufe innerhalb der Verwaltung ändern.

Der Datenschutz als Anwalt des Bürgers für den Schutz seines Rechts auf informationelle Selbstbestimmung bietet sich hier als Partner an. Elektronische Verwaltung muss auch in dieser Beziehung die Rechte der Bürger wahren. Nur bei Wahrung des Rechts auf informationelle Selbstbestimmung wird der Bürger das notwendige Vertrauen in diese neuen Angebote haben. Dazu gehört einmal die Sicherung von Vertraulichkeit, Verfügbarkeit und Integrität der Datenverarbeitung, dazu gehört aber auch, dass von diesen Vorgängen nur die dazu gesetzlich Berechtigten Kenntnis erhalten. Verschlüsselung und elektronische Signatur sind hier unverzichtbar.

Noch größeres Gewicht erhalten die Datenschutzfragen dadurch, dass verschiedene Projekte - u.a. der **„Virtuelle Marktplatz Bayern“** auf Initiative der Bayer. Staatsregierung - ein kombiniertes Angebot von öffentlichen und privaten Dienstleistungen vorsehen. Hier ist eine sichere Trennung der einzelnen Datenflüsse in dem Sinn erforderlich, dass nicht der einzelne Dienstleistungsanbieter von für ihn interessanten Verwaltungsvorgängen erfährt. Daten der Verwaltung dürfen nur auf den dazu vorgesehenen Rechnern der Verwaltung verarbeitet und gespeichert werden. Es muss auch sichergestellt sein, dass nicht beim Betreiber eines zentralen Servers ein elektronisches Abbild des Nutzerverhaltens des Bürgers und der Bürgerin entsteht. Schließlich

sind die Verantwortlichkeiten für die einzelnen Datenverarbeitungsvorgänge klarzustellen.

Ich habe in dieser Richtung bereits mit Schreiben vom 7. Februar des Jahres zahlreiche Fragen und Hinweise an die Bayer. Staatskanzlei gestellt bzw. gegeben, eine abschließende Antwort aber bis Redaktionsschluß dieses Berichts nicht erhalten. Ich konnte deshalb bis dahin noch kein Urteil darüber abgeben, ob Datenschutz und Datensicherheit beim „Virtuellen Marktplatz Bayern“ gewährleistet sind (Nr. 8.4).

Nach Übermittlung des Vorabdrucks dieses Berichts an den Beirat beim Landesbeauftragten für den Datenschutz (ab 1.12. Datenschutzkommission beim Bayer. Landtag) zur Vorberatung gem. Art. 30 Abs. 5 Satz 3 BayDSG führte die Staatskanzlei mit Schreiben vom 1. Dez. 2000 aus, dass „ im derzeitigen Ausbauzustand“ ein reines Informationsangebot der Behörden geplant sei und personenbezogene Daten der Benutzer „weder im VMB auf privat betriebenen Rechnern gespeichert noch .....ein Datenfluss über Rechner des VMB (erfolge)“ Beigelegt war eine allgemeine Beschreibung der Datenflüsse im Baynet, in der u.a. ausgeführt wird, dass die IP-Adresse des Besuchers nicht gespeichert werde, und Nutzungsprofile, soweit diese erforderlich seien, nur in anonymisierter Form erstellt würden.

In der kurzen Zeit bis zur Beratung im Beirat am 5.12.2000 und zur Übergabe des Berichts am 14.12. war es mir nicht möglich, diese Angaben im einzelnen zu überprüfen. Ich muß mir eine endgültige Bewertung deshalb nach wie vor vorbehalten.

Generell darf **elektronische Verwaltung nicht zum gläsernen Bürger** für die Verwaltung führen. Als wesentliches Hilfsmittel zur Erreichung dieses Ziels bieten sich die Nutzung von Datenschutz sichernden Techniken, wie Anonymisierungs- und Pseudonymisierungsverfahren, sowie die strenge Beachtung des Erforderlichkeitsprinzips, insbesondere des Grundsatzes der Datensparsamkeit an. Ich habe in einer Arbeitsgruppe der Datenschutzkonferenz mitgearbeitet, die zu diesem Fragenkreis Orientierungshilfen erarbeitet hat, die in Kürze veröffentlicht werden (Nr. 8.5). Ich werde sie dann auch auf meiner Website bereithalten. Bereits zur Verfügung stehen Orientierungshilfen für „Grundsätze für Benutzerrichtlinien für den Umgang mit dem Internet“ (www.datenschutz-bayern.de/technik/orient/ibenrili.htm), für „Veröffentlichung von Informationen im Internet und Intranet“ (www.datenschutz-bayern.de/technik/orient/int-publ.htm) und

schließlich die „Online-Datenschutz-Prinzipien (ODSP)“ (http://www.datenschutz-bayern.de/technik/orient/priv_pol.htm). Dazu kommen die Orientierungshilfe „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ (www.datenschutz-bayern.de/technik/orient/int_gesch.pdf) des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und meine Hinweise zur „Datensicherheit beim Betrieb eines Landkreisbehördennetzes (Intranet)“ (www.datenschutz-bayern.de/technik/orient/landk_g.pdf).

1.1.3 Neue Lösungsansätze? Neue Lösungsansätze!

Im letzten Tätigkeitsbericht, dem 18., hatte ich unter Nr. 1.1 gefordert, dass die Umsetzung der EG-Richtlinie über den Datenschutz, Rl 95/46/EG, zum Anlass genommen wird, im **neuen Datenschutzrecht** auf die Entwicklung der letzten 20 Jahre einzugehen. U.a. habe ich Regelungen über Chipkarten, Video-Anwendungen, sowie über Prinzipien des modernen Datenschutzes wie Grundsätze der Datensparsamkeit, der Möglichkeit der Anonymisierung sowie des Verwendens von Pseudonymen gefordert. Weiter habe ich festgestellt, dass ich mich neben meiner Funktion als Kontrollinstanz wesentlich auch als „Dienstleistungsbetrieb Datenschutz“ sowie als Anwalt der Bürger verstehe (Nr. 1.1 des 18. TB.).

In der inzwischen im Wesentlichen in Kraft getretenen **Novelle zum Bayer. Datenschutzgesetz** wurde diesen Forderungen bedauerlicherweise nicht Rechnung getragen. Im Entwurf zur Novelle des Bundesdatenschutzgesetzes sind immerhin Regelungen zur Videobeobachtung sowie zur Datensparsamkeit und der Anonymisierung bzw. Pseudonymisierung enthalten. Während der Beratung wurden auch aus der Mitte des Landtages zu diesen Gebieten Vorschläge eingebracht. Die Staatsregierung hat eine weitere Prüfung angekündigt, inwieweit im Bayerischen Datenschutzgesetz Regelungen zu Video-Anwendungen, Chipkarten, Anonymisierung und Pseudonymisierung sowie eine Neufassung der Vorschriften über technische und organisatorische Maßnahmen zur Datensicherheit notwendig sind.

Ich bedauere, dass die Gelegenheit zur Anpassung des Bayer. Datenschutzgesetzes an die Anforderungen der neuen Datenverarbeitungswelt, aber auch zur weiteren Verbesserung von Aus-

kunftsregelungen nicht genutzt wurde. Ich muss dabei allerdings einräumen, dass der Zeitdruck wegen der abgelaufenen Umsetzungsfrist der EG-Richtlinie hoch war. Auch hat die Bundesregierung, an deren Gesetzentwurf sich das Bayer. Datenschutzgesetz verständlicherweise als Modell ausgerichtet hat, jedenfalls die Chipkartenregelung und die ebenfalls notwendige Neuregelung der technischen Anforderungen auf eine „zweite Stufe“ der Neuregelung des Datenschutzrechtes verschoben. Ich meine allerdings, dass wenigstens die Grundsätze der Datensparsamkeit und die Forderungen nach Vorrang von anonymen oder pseudonymen Datenverarbeitungsverfahren, die auch im öffentlichen Bereich ihre Berechtigung haben, wie auf Bundesebene auch in Bayern in die jetzige Realisierungsstufe hätten aufgenommen werden können.

Auf Bundesebene wurde die zweite Stufe mit der Beauftragung von Gutachtern und der Einrichtung von Expertengremien inzwischen auf den - möglicherweise sehr langen Weg - gebracht. Ich hoffe, dass die notwendige „zweite Stufe“ in Bayern in absehbarer Zeit realisiert wird. Die Staatsregierung hat während des Gesetzgebungsverfahrens signalisiert, dass sie die „zweite Stufe“ noch in dieser Legislaturperiode in Angriff nehmen wird.

Zu begrüßen ist, dass die Beschränkung meiner Kontrollmöglichkeiten bei nur in Akten befindlichen Vorgängen auf die sog. Anlasskontrolle endlich weggefallen ist. Weiterhin ist hervorzuheben, dass nunmehr alle öffentliche Stellen, die automatisierte Verfahren mit personenbezogenen Daten einsetzen, behördliche Datenschutzbeauftragte zu bestellen haben. Daneben enthält das neue Bayerische Datenschutzgesetz punktuelle Verbesserungen. Als eine Stärkung des Datenschutzes sehe ich auch die Umbenennung des "Beirats beim Landesbeauftragten für den Datenschutz" in eine "Datenschutzkommission beim Landtag" bei gleichen Aufgaben dieses Gremiums an. Als Datenschutzkommission hat das Beratungsorgan noch größeres Gewicht bei der Unterstützung des Landesbeauftragten. Zum ganzen verweise ich unten auf Nr. 2.2.2 dieses Berichts.

In Bezug auf den „Dienstleistungsbetrieb Datenschutz“ beteilige ich mich mit Zustimmung des Herrn Landtagspräsidenten an einem interessanten Projekt, das mein Kollege in Schleswig-Holstein, Dr. Helmut Bäumler, auf den Weg gebracht hat, das aber nach seiner Konzeption als **gemeinsames Projekt „Virtuelles Datenschutzbüro (vDSB)“** der teilnehmenden Datenschutz-

kontrollstellen zu verstehen ist. Das Projekt soll die Präsenz der Datenschutzbeauftragten im Internet und ihre Kompetenz in Fragen des Internets entscheidend verbessern, sowie die Zusammenarbeit der Datenschutzbeauftragten erleichtern und ebenfalls verbessern.

In dem Projekt werden Datenschutzverantwortliche und Datenschutzinteressierte auf nationaler und internationaler Ebene virtuell, d.h. über das Netz zusammenarbeiten und den Bürgerinnen und Bürgern sowie allen Interessierten als Ansprechpartner zur Verfügung stehen. Es werden zusammengefasst vier Zielebenen verfolgt:

- Bildung einer Kommunikationsplattform
    - Verbesserung der Zusammenarbeit von Datenschutzinstanzen, insbesondere nationalen und internationalen Datenschutzbeauftragten, durch thematische Verteilerlisten und Diskussionsplattformen. Im Hinblick auf die Internationalität der Datenverarbeitung, insbesondere über das Internet, ist auch eine internationale Zusammenarbeit der Datenschutzbeauftragten notwendig.
- Meinungsaustausch mit externen Experten; Beteiligung an und Anregung von Diskussionen im Netz
- Zentrale Ansprechplattform für Bürgerinnen und Bürger; Es soll die Möglichkeit gegeben werden, Antworten auf oft gestellte Fragen zu erhalten („FAQ“); bei Fragen, die einzelne Datenschutzbeauftragte betreffen, sollen sie komfortabel zu den zuständigen Stellen weitergeleitet werden; das vDSB soll eine Ansprechplattform für Medien und Wirtschaft sein
- Veröffentlichungsmedium; zentrale Möglichkeit für die Mitglieder des vDSB („Projektpartner“), ihre Beiträge ins Netz zu stellen bzw. auf bereits vorhandene lokale Beiträge zu verweisen und sie damit über eine zentrale Adresse der (globalen) Netzgemeinde zu präsentieren
- Praktizierung und Praxiserprobung von datenschutzfreundlichen Techniken („Privacy Enhancing Technologies - PET“) mit der Möglichkeit der Rückkopplung gegenüber den Entwicklern und Herstellern von PET.

Interessiert an einer Beteiligung an dem Projekt als Mitträger haben sich bis jetzt fast alle deutschen Datenschutzbeauftragten gezeigt einschließlich des Bundesbeauftragten,

sowie die Niederländische Registratiekammer, der Züricher Beauftragte für den Datenschutz, die Datenschutzbeauftragte von Ontario/Canada und der Datenschutzbeauftragte der katholischen Kirche Norddeutschlands.

Ich halte das Projekt für außerordentlich interessant. Es wird die Präsenz der Datenschutzbeauftragten im Internet und die Zusammenarbeit der teilnehmenden Datenschutzbeauftragten auf nationaler und internationaler Ebene grundlegend verbessern und gegenüber der mehr punktuellen Zusammenarbeit im Rahmen von nationalen und internationalen Konferenzen erweitern. Weiter wird die Mitarbeit im vDSB die technische Kompetenz durch Praktizierung von datenschutzfreundlichen Techniken, ständige Beteiligung an Diskussionen über diese Fragen und die in diesem Zusammenhang entstehende Rückkopplung ebenfalls wesentlich verbessern.

Diese Verbesserungen sind insbesondere auch deshalb notwendig, da sich auch die Daten verarbeitenden Stellen untereinander immer mehr vernetzen. Ich darf in diesem Zusammenhang wiederum auf das Projekt „Virtueller Marktplatz Bayern“, sowie auf das Projekt des Bundesinnenministeriums eines generellen Portals der öffentlichen Verwaltungen in Deutschland Bezug nehmen, das unter der Internetadresse http://www.staat-modern.de/infos/adressv/index.htm erreichbar ist. Mit letzterem Projekt soll ein erster Schritt zu einem „bundesweiten Verwaltungsportal im Internet“ getan werden. Auch angesichts dieser Tendenzen halte ich die geplante Vernetzung der Datenschutzbeauftragten in einem „virtuellen Datenschutzbüro“ für einen konsequenten und notwendigen Schritt.

1.2 Übersicht über meine Tätigkeit im Berichtszeitraum (anhand einer Auswahl wesentlicher Einzelfeststellungen)

1.2.1 Polizeibereich

Im Polizeibereich habe ich mich im Berichtszeitraum mit ähnlichen Problembereichen beschäftigen müssen wie in den vergangenen Jahren. Teilweise konnte ich in den Verhandlungen mit dem Innen- und Justizministerium Fortschritte erzielen (wobei ich auf Antworten des Innenministeriums oft sehr lange warten muss), teilweise treten die Verhandlungen aber auf der Stelle. Hervorzuheben sind:

Polizeiliche Datensammlungen, insbesondere Kriminalaktennachweis (KAN)

Verbesserungen konnten insbesonders in folgenden Bereichen auf den Weg gebracht werden, wobei die Umsetzung in den Richtlinien noch aussteht:

- Für Fälle geringerer Bedeutung sollen in Zukunft allgemein – nicht nur in den in den Richtlinien genannten wenigen Fällen – auch geringere Speicherfristen festgelegt werden können, als die Regelfristen von 10 Jahren. Damit wird z.B. für eine Schwarzfahrt nicht mehr eine Speicherfrist von 10 Jahren festgelegt werden müssen (Nr. 5.3.1.4).

- Die endgültige Entscheidung der Polizei über die Eintragung in den KAN soll nicht mehr schon bei Aufnahme der polizeilichen Ermittlungen getroffen werden, sondern erst bei deren Abgabe an die Staatsanwaltschaft. Auch spätere Hinweise und Erkenntnisse sollen berücksichtigt werden. Dadurch soll die Gefahr vermindert werden, dass Eintragungen ohne ausreichenden Tatverdacht erfolgen, was ich im letzten Tätigkeitsbericht (vgl. Nr. 5.3.1.1, 18. TB) feststellen musste (Nr. 5.3.1.1).

- Die Polizei soll auch dann seitens der Staatsanwaltschaft vom Wegfall des Tatverdachts gegen einen Beschuldigten unterrichtet werden, wenn dieser nicht zu benachrichtigen war, weil er z.B. nicht als Beschuldigter vernommen wurde. Bisher erfolgte eine solche Mitteilung nicht, so dass die Polizei vom Wegfall des Tatverdachts nichts erfuhr. Auch dieser Effekt führte zu unberechtigten Speicherungen (Nr. 5.3.1.1).

Offen sind meine Forderungen, die sich an die Justiz richten, wegen des Sachzusammenhangs aber bereits hier Erwähnung finden sollen:

- Unterrichtung der Polizei von entlastenden Ermittlungsergebnissen der Staatsanwaltschaft in jedem Fall; die Polizei hätte dadurch eine bessere Möglichkeit zu einer Überprüfung ihrer Eintragungsentscheidung (Nr. 5.3.1.1).

- Der Betroffene wird von der Einstellung der Ermittlungen nicht in jedem Fall unterrichtet, in dem der Tatverdacht entfallen ist oder sich seine Unschuld herausgestellt hat. Damit entfällt für ihn die Möglichkeit, sich gegen eventuelle Speicherungen bei der Polizei zu wehren (Nr. 5.3.1.1).
  Das Staatsministerium der Justiz hat beide Forderungen abgelehnt.

Im Übrigen hebe ich folgende Mängel oder Problemkreise hervor:

- In einer Polizeidirektion waren Ordnungswidrigkeiten als alleinige Unterlage im KAN gespeichert, was unzulässig war. Die Speicherungen wurden gelöscht (Nr. 5.3.1.4).

- Der personengebundene Hinweis „Geisteskrank“ wurde wiederum gespeichert, ohne dass die Voraussetzungen – ärztliche Feststellung der Geisteskrankheit – vorgelegen hätten. Ich erwarte, dass das Innenministerium durch entsprechende Hinweise dafür sorgt, dass ich nicht bei jeder Prüfung wieder den gleichen Fehler rügen muss (Nr. 5.3.1.5).

- Es ist in Einzelfällen eine Tendenz zu beobachten, den Zugriff auf so genannte „Lagedateien“ für alle Polizeibeamten präsidiumsweit bis bayernweit zu eröffnen. Im Unterschied zum Kriminalaktennachweis sind in den Lagedateien auch andere Personen als Beschuldigte aufgenommen, wie Zeugen, Anzeigeerstatter, Opfer, Mitteiler, Kontaktpersonen u.a.. Eine präsidiums- oder gar bayernweite Recherche nach diesen Personen halte ich vom Zweck einer Lagedatei, nämlich Auskunft über die polizeiliche Lage auf regionaler Ebene zu geben, nicht für gedeckt. Ich hielte eine solche Entwicklung für bedenklich (Nr. 5.4.1).

- In einem Präsidium sollten in einer Datei über vorgetäuschte Verkehrsunfälle auch die anwaltschaftlichen Vertreter von Tatverdächtigen wegen deren Forderungen gespeichert werden. Auf meine Rüge dieser pauschalen Speicherung von Rechtsanwälten erfolgt eine solche nicht mehr, sondern nur dann, wenn der Anwalt ebenfalls als Tatverdächtiger anzusehen ist (Nr. 5.4.2).

- Das Auskunftsrecht über Datenspeicherungen ist eine zentrale Grundlage des Rechts auf informationelle Selbstbestimmung. Damit ist die Praxis des Innenministeriums nicht vereinbar, für einen ganzen Deliktsbereich, den unbefugten Rauschgifthandel, das Auskunftsrecht aus Art. 48 PAG generell auszuschließen. Verhandlungen mit dem Innenministerium waren bisher erfolglos. Ich erwäge insoweit eine Beanstandung des Ministeriums (Nr. 5.8.3).

- Mehrfach rügen musste ich eine mangelhafte bzw. zu späte Beteiligung durch das Innenministerium, beispielsweise bei der DNA-Analyse-Datei, der Verbunddatei VICLAS und der Verbunddatei Arbeitsdatei PIOS-Rauschgift. Ich habe deshalb an den Amtschef des Innenministeriums geschrieben, der eine zu späte Beteiligung als Büroversehen erklärte. Eine rechtzeitige Beteiligung ist eine meiner wesentlichen Arbeitsgrundlagen. Ich muss sie deshalb in jedem Fall einfordern. Auch erwarte ich, dass auf meine Bedenken sachlich eingegangen wird, wenn ihnen nicht Rechnung getragen wird (Nr. 5.10).

- Zuletzt hebe ich noch einen ungewöhnlichen Einzelfall hervor, der wohl auf Übereifer in einer grundsätzlich guten Sache zurückzuführen ist: Im Bereich einer Polizeidirektion wurde ein Bürger dem Gesundheitsamt als „Suchtgefährdeter“ gemeldet, weil bei ihm innerhalb eines Zeitraums von knapp zweieinhalb Jahren bei vier Kontrollen jeweils Anzeichen von Alkoholkonsum festgestellt worden war. Die in drei Fällen durchgeführte Alkoholkontrolle ergab jeweils Werte unter der Ordnungswidrigkeitengrenze. Auf meine Drohung mit einer Beanstandung erging eine Anweisung, entsprechende Meldungen erst bei nachweislicher Suchtgefährdung bzw. -abhängigkeit vorzunehmen (Nr. 5.7.2).

1.2.2 Verfassungsschutz

In diesem Bereich habe ich bei meinen Prüfungen im Wesentlichen keine grundsätzlichen Mängel feststellen müssen. Insbesonders hat die umfangreiche Prüfung des Vorwurfs, beim Landesamt für Verfassungsschutz würden „Dossiers“ über demokratische Politiker geführt, keine Hinweise auf die Berechtigung eines solchen Vorwurfs ergeben. Dabei wurden von mir und meinen Mitarbeitern in mehrwöchigem Einsatz sämtliche Dateien überprüft, eingeschlossen wurden die Aktenbestände in den Registraturen einschließlich der gesondert aufbewahrten Geheimakten. Zu kritisieren war in einem Fall die Aufnahme eines Quellenberichts mit für die Aufgabenerfüllung nicht erforderlichen Angaben über das Intimleben einer Person sowie eine zu lange Aufbewahrung einer Vielzahl von Akten, die bereits dem Archiv hätte angeboten werden oder ausgesondert werden müssen (Nr. 6.2.1).

Meiner Kritik wurde Rechnung getragen, insbesondere wurde inzwischen eine entsprechende Vereinbarung mit dem Staatsarchiv abgeschlossen (Nr. 6.2.4).

Zu bemängeln war schließlich, dass die Speicherfristen in mehreren Fällen nicht wie vorgeschrieben vom Ereigniszeitpunkt ab berechnet wurden, sondern vom Zeitpunkt der Kenntnis des LfV vom Ereignis, was zum Teil zu einer mehrjährigen Verlängerung der Speicherungen führte. Das Abstellen dieses Fehlers, den ich schon bei vergangenen Prüfungen feststellen musste, wur-

de zugesichert, die fehlerhaften Speicherungen wurden berichtigt bzw. gelöscht (Nr. 6.2.2).

1.2.3 Wesentliches aus dem Bereich der Justiz

Hervorzuheben sind hier einzelne Grundsatzprobleme und einige Stellungnahmen zu Gesetzgebungsverfahren und Richtlinien.

Über die **Weigerung des Justizministeriums, bei Wegfall des Tatverdachts ein besonderes Interesse des Beschuldigten an der Mitteilung der Einstellung des Verfahrens anzuerkennen**, habe ich wegen des Sachzusammenhangs bereits unter dem Abschnitt Polizei berichtet. Das Gleiche gilt für die Ablehnung seitens der Justiz, der Polizei regelmäßig entlastende Momente mitzuteilen, die sich durch zusätzliche Ermittlungen seitens der Staatsanwaltschaft im Laufe eines später eingestellten Strafverfahrens ergeben haben.

Ich bedauere diese Haltung. Sie verschlechtert sowohl die Möglichkeit des Betroffenen, gegen die Speicherung seiner Daten in polizeilichen Dateien vorzugehen, als auch die Entscheidungsgrundlagen der Polizei für die Frage, ob die Daten des Betroffenen nach Einstellung des Verfahrens weitergespeichert werden sollen. Das Innenministerium wäre zu einer nochmaligen Überprüfung der Speicherung in diesen Fällen bereit. Das setzt aber voraus, dass die Polizei von diesen Fällen überhaupt erfährt. Ich verweise zum Ganzen nochmals auf die Nr. 5.3.1.1.

Im Gegensatz zur gesetzlichen Regelung wird in Bayern bei der **präventiven DNA-Analyse** vordringlich mit einem „Einverständnis“ des Betroffenen gearbeitet. Die gesetzliche Regelung sieht dagegen vor, dass die DNA-Analyse zur vorbeugenden Verbrechensbekämpfung unter bestimmten gesetzlichen Voraussetzungen von einem Richter angeordnet wird.

Mit einer DNA-Analyse nach regelmäßigen „freiwilligem Einverständnis“ des Betroffenen wird dieser gesetzlich vorgesehene Schutzmechanismus umgangen. Kein Richter prüft, ob der Betroffene schwere Straftaten im Sinn der gesetzlichen Regelung begangen hat, kein Richter prüft, ob bei ihm die Gefahr weiterer schwerer Straftaten besteht. Das Staatsministerium der Justiz und das Staatsministerium des Inneren waren trotz meiner eindringlichen Vorhaltungen nicht bereit,

von dieser gesetzesumgehenden Praxis abzugehen. Von einer förmlichen Beanstandung habe ich bis jetzt nur deshalb abgesehen, weil auch in der Rechtsprechung umstritten ist, ob das „freiwillige Einverständnis“ ausreichend ist (Nr. 7.2.3.1).

In einem Einzelfall hat sich ein Gericht geweigert, einem Bürger **Einsicht in die Akten seines bereits abgeschlossenen Betreuungsverfahrens** zu gewähren. Der Bürger habe dazu kein berechtigtes Interesse glaubhaft gemacht.

Ich hebe diesen Fall hervor, weil er ein kaum glaubliches Unverständnis in die Situation eines Betroffenen offen legt, der die Einzelheiten eines ihn in seinem innersten Kreis betreffenden Verfahrens kennen will, und ich nicht ausschließen kann, dass auch bei anderen öffentlichen Stellen ein derartiges Unverständnis besteht.

Die Akteneinsicht wurde nach meiner Intervention gewährt (Nr. 7.3.2).

Die Praxis des **„großen Lauschangriffs“** soll nach dem Grundgesetz wegen ihrer großen Eingriffsintensität parlamentarisch kontrolliert werden. Das bayerische Ausführungsgesetz dazu sieht diese Kontrolle in dem geheim tagenden „Parlamentarischen Kontrollgremium“ vor. Ich habe für eine effektive Kontrolle eine öffentliche Behandlung der grundsätzlichen Erfahrungen mit diesem sehr eingreifenden Verfahren gefordert, von dem nicht nur wenige Beschuldigte, sondern auch zahlreiche nicht Betroffene berührt sein können. Im Gesetz wurde diese Forderung leider nicht berücksichtigt. Ich halte sie zu einer effektiven Kontrolle für unverzichtbar (Nr. 7.1.3).

Schließlich hebe ich noch zwei aus meiner Sicht positive Beispiele hervor, in denen Forderungen des Datenschutzes Rechnung getragen wurde:

Die **Presserichtlinien des Bayer. Justizministeriums** wurden inzwischen fertig gestellt. Dabei wurde meinen Anregungen weitgehend Rechnung getragen, zuletzt meinen Forderungen nach einer nur ausnahmsweisen Weitergabe personenbezogener Daten bei einer Berichterstattung aus Strafverfahren und nach einer wegen der Unschuldsvermutung restriktiven Handhabung einer

aktiven Öffentlichkeitsarbeit. Die Veröffentlichung steht bevor (Nr. 7.3.3).

Das **Bundesjustizministerium** hat einer Forderung des Datenschutzes nach einer Effizienzprüfung der staatlichen Telefonüberwachungsbefugnisse durch Vergabe eines Forschungsvorhabens entsprochen (Nr. 7.2.4.4).

1.2.4 Bereich Kommunen und Einwohnermeldewesen

Neben den schon aus den vorherigen Tätigkeitsberichten bekannten Problemen wie Datenschutz bei Bürgerbegehren, Videoüberwachung, Weitergabe interner Beratungsunterlagen an die Presse und von Melderegisterdaten an Adressbuchverlage, habe ich mich mit Fragen der Modernisierung der Verwaltung durch Nutzung von Intranet und Internet beschäftigt. Im Einzelnen hebe ich hervor:

Das Orientierungspapier **„Vom Bürgerbüro zum Internet – Empfehlungen für eine bürgerfreundliche Verwaltung“**, das eine Arbeitsgruppe der Datenschutzkonferenz, an der ich teilgenommen habe, unter der Federführung meiner Kollegin in Nordrhein-Westfalen, Bettina Sokol, verfasst hat. Darin werden Hinweise gegeben u.a. zur datenschutzgerechten Gestaltung von Bürgerbüros, Callcentern, zu Informationsangeboten öffentlicher Stellen im Internet, zur Bürgerkarte und allgemein zur interaktiven Verwaltung. Das Orientierungspapier, das in Kürze veröffentlicht wird, gibt Hinweise zu den technisch-organisatorischen Anforderungen an eine sichere Kommunikation zwischen Bürger und Verwaltung und Hinweise für die datenschutzgerechte Gestaltung und technische Absicherung der Informationsangebote (Nr. 8.5).

Datenschutz bei Bürgerbegehren macht immer noch einigen Bürgermeistern Schwierigkeiten, obwohl wir auch während des Jahres immer wieder auf diese Fragen hinweisen. Namen und Anschriften in den Eintragungslisten unterliegen ab Abgabe der Liste an die Gemeinde den für diese geltenden Datenschutzbestimmungen. Insbesondere dürfen diese Angaben ausschließlich für die Feststellung der Zulässigkeit des Bürgerbegehrens genutzt werden und nicht an Dritte weitergegeben werden (Nr. 8.6).

Die **Führung zentraler Adressdateien in Gemeinden** muss datenschutzgerecht erfolgen. Sie darf nicht dazu führen, dass Vorschriften z.B. des Steuer- oder Sozialgeheimnisses dadurch umgangen werden, dass Daten aus diesen Verfahren wegen ihres unbeschränkten Online-Zugriffs auch Bediensteten anderer Stellen der Gemeinde offen stehen, ohne dass sie nach den einschlägigen Vorschriften dazu berechtigt wären. Das Gleiche gilt für sonstige Daten, wie z.B. die Bankverbindung, wenn deren Kenntnis für den jeweiligen Sachbearbeiter nicht erforderlich ist (Nr. 8.7).

Die **Weitergabe von Melderegisterdaten** an Adressbuchverlage ist immer wieder Gegenstand von Bürgerbeschwerden. Ich musste mich dabei darauf beschränken, die Bürger auf ihr Widerspruchsrecht gegen die Weitergabe von bestimmten Melderegisterdaten, die nach dem Melderecht zulässig ist, hinzuweisen. Eine Empfehlung der Konferenz der Datenschutzbeauftragten, im Melderechtsrahmengesetz für die Weitergabe dieser Daten das Einverständnis des Betroffenen vorzusehen, wurde leider von der Bundesregierung nicht aufgegriffen (Nr. 9.1).

Das **Adoptionsgeheimnis** wurde in zwei schwer wiegenden Fällen verletzt. Der Geburtsname war in beiden Fällen im Einwohnermelderegister entgegen dem Gebot noch enthalten, nicht mehr benötigte Daten zu löschen. Die Geburtsnamen wurden im Online-Verfahren an die Polizei übermittelt und von dieser den Betroffenen entgegengehalten. Es bedarf keiner weiteren Ausführungen, welch schwer wiegende Folgen damit verbunden sein können. Ich habe diese Verstöße beanstandet.
Ich empfehle allen Gemeinden, ihre Melderegister auf derart unzulässige Speicherungen zu überprüfen (Nr. 9.3).

1.2.5 Gesundheitswesen

Im Gesundheitswesen waren wiederum u.a. Fragen der datenschutzgerechten Ausgestaltung von Forschungsvorhaben, der Datenverarbeitung in Klinikinformationssystemen, des Outsourcings der Verarbeitung von Patientendaten und der Telemedizin von besonderer Bedeutung.

Allgemeine Grundsätze **zur datenschutzgerechten Ausgestaltung von Forschungsvorhaben** habe ich in meinem Beitrag Nr. 2.3.1 formuliert. Hervorzuheben ist der Vorrang der anonymisierten, erforderlichenfalls pseudonymisierten Datenverarbeitung, das Erfordernis einer Rechtsgrundlage oder einer informierten Einwilligung bei der Verarbeitung von personenbezogenen Daten und der Vorrang des Arztgeheimnisses vor den Befugnissen aus dem allgemeinen Datenschutzrecht.

Die Anwendung dieser Grundsätze auf eine Reihe von Forschungsvorhaben hat gezeigt, dass sich die datenschutzgerechte Ausgestaltung und das Forschungsziel bei Zusammenarbeitsbereitschaft beider Seiten durchaus vereinigen lassen. Als Beispiele nenne ich die **„Prospektive Analyse der Drogentoten in Bayern 1999“** (Nr. 3.2.1) und die **Forschungsstudie „Plötzlicher Säuglingstod“** (Nr. 3.2.2), bei denen rechtzeitig mit mir Kontakt aufgenommen wurde, so dass ein beiderseits befriedigendes Ergebnis erreicht wurde.

Leider gibt es auch gegenteilige Beispiele, in denen ich zu spät eingeschaltet wurde (PISA-Schulleistungsstudie der OECD (Nr. 2.3.2.1) und „IEA-Studie Civic Education“ (Nr. 2.3.2.2). In diesen beiden Fällen mussten die Forderungen des Datenschutzes nach u.a. informierter, freiwilliger Einwilligung der Betroffenen und ausreichender Anonymisierung erst in einem sehr späten Stadium nachverhandelt werden.

Für die **Datenverarbeitung in Klinikinformationssystemen** wurde im Zuge meiner Prüfung eines Krankenhauses ein abgestuftes System von Zugriffsberechtigungen anhand der unterschiedlichen medizinischen Notwendigkeiten weiterentwickelt, das einerseits den Bedürfnissen des Krankenhauses Rechnung trägt, andererseits aber auch das grundsätzlich auch innerhalb eines Krankenhauses geltende Arztgeheimnis (gegenüber nicht behandelnden Einheiten) berück-

sichtigt (Nr. 3.4.1). Das Konzept geht von dem Grundsatz aus, dass Ärzte und sonstiges Fachpersonal in den Abteilungen, für die sie regelmäßig tätig sind, im jeweils erforderlichen Umfang Zugriff auf die Behandlungsdaten haben. Weiter ist eine Zugriffsberechtigung mit Begründungszwang z.B. für Notfälle vorgesehen. Wegen der auch für längere Zeit nach der Entlassung des Patienten für das Krankenhauspersonal bestehenden Zugriffsberechtigungen auf die Stammdaten habe ich eine Einschränkung auf einen Kerndatensatz gefordert, was vom Krankenhaus aufgegriffen wurde.

Zum **Outsourcing der Mikroverfilmung von Patientendaten** musste ich gegenüber zwei Krankenhäusern auf Art. 27 Abs. 4 des Bayer. Krankenhausgesetzes verweisen, der eine Verarbeitung von Gesundheitsdaten nur durch andere Krankenhäuser vorsieht, in keinem Fall aber bei Privaten. Diese Vorschrift hat wegen des anderweitig nicht gegebenen Schutzes der medizinischen Daten durch Arztgeheimnis, strafprozessuales Beschlagnahmeverbot und Zeugnisverweigerungsrecht ihren guten Sinn. Ihre Einhaltung musste durch eine Beanstandung sichergestellt werden (Nr. 3.4.2).

Mit **Fragen der Telemedizin** habe ich mich in zahlreichen Vorträgen und Beratungsgesprächen beschäftigt. Als Grundsatz habe ich dabei herausgestellt, dass in der Telemedizin die gleichen Anforderungen an die Verarbeitung von Patientendaten gelten, wie in der traditionellen Medizin. Als Schlagwort kann gesagt werden: „Technik ersetzt keine fehlenden Datenverarbeitungsberechtigungen“. Zu beachten ist die ärztliche Schweigepflicht, die grundsätzlich auch gegenüber anderen, nicht behandelnden Ärzten gilt, sowie der daraus folgende Grundsatz, dass für die Übermittlung von Patientendaten entweder eine dazu berechtigende Norm oder aber, abgesehen von Notfällen, die informierte Einwilligung des Patienten erforderlich ist. In diesem Sinn habe ich mich mit den Projekten „Telemedizin in Ostbayern“ und „Neue Kommunikationstechnologien in der Notfallmedizin (NOAH II)“ befasst (Nrn. 3.5 und 3.6).

Die **unzulässige Verarbeitung von Daten Behinderter in einem Universitätsklinikum** stellte einen besonders spektakulären Einzelfall dar (Nr. 3.10). Ich habe diese Verarbeitung beanstandet, da eine Einwilligung zur Datenübermittlung vom ärztlichen Dienst des Behindertenheims an das Universitätsinstitut zur genetischen Untersuchung des Blutes der Betroffenen nicht vorgele-

gen hatte.

1.2.6 Personaldaten

Im Bereich der Verarbeitung von Personaldaten habe ich mich u.a. mit der geplanten Möglichkeit der Auslagerung der Beihilfesachbearbeitung auf andere Stellen als auf Krankenversicherungen (z.B. GmbH) befasst (Nr. 12.1.1). Ich habe dagegen im Gesetzgebungsverfahren grundsätzliche Bedenken erhoben, weil dort, anders als bei Krankenversicherungsunternehmen, eine strafrechtlich gesicherte Verschwiegenheitspflicht nicht besteht. Weiter habe ich ein an die öffentlichen Stellen angelehntes Akteneinsichtsrecht, Aufbewahrungsbestimmungen sowie eine Unterstellung unter meine Kontrollbefugnis gefordert. Sämtlichen Forderungen wurde nicht Rechnung getragen. Auf diese ausgelagerten Datenverarbeitungen sollen daher nur die weniger weit gehenden Datenschutzvorschriften des Bundesdatenschutzgesetzes für den privaten Bereich Anwendung finden, wenn diese zumindest in nicht-automatisierten Dateien erfolgen. Ist das nicht der Fall, also bei einer ausschließlichen Verarbeitung in Akten, ist nicht einmal das Bundesdatenschutzgesetz anwendbar. Ich bedauere deshalb die nunmehr gegebene Möglichkeit der Auslagerung der Beihilfesachbearbeitung auf Private, die nicht Krankenversicherungsunternehmen sind, als einen ausgesprochenen Rückschritt hinsichtlich des Datenschutzes in diesem sensiblen Bereich. Ich hoffe, dass die Aufsichtsbehörden die weitere Entwicklung kritisch beobachten.

1.2.7 Technik und Organisation

Die Schwerpunkte im Bereich Technik und Organisation waren neben Beratung, regelmäßigen und anlassbezogenen Prüfungen, die Behandlung von Grundsatzthemen zur Sicherheit in verteilten Netzen und zur Realisierung datenschutzrechtlicher Forderungen auch angesichts der neuen Möglichkeiten der IuK-Technik und mit Hilfe dieser Technik. Besonders hervorzuheben sind:

Zur **Sicherheit im Bayerischen Behördennetz** sind seit dem letzten Bericht Fortschritte, aber noch kein Durchbruch zu vermelden. Lange Zeit wurde von den verschiedenen Gremien mit der

Diskussion über die zu verwendenden Protokolle verbracht. Eine von mir angeregte Übergangslösung für sichere e-mail auf der Basis von PGP wurde im Hinblick auf eine erwartete Dauerlösung zunächst nicht verfolgt. Die Dauerlösung konnte aber auch noch nicht realisiert werden. Als Ergebnis nach fünfjähriger Diskussion steht nun eine Zertifizierungsstelle im Landesamt für Statistik und Datenverarbeitung und entsprechend meiner seit langem erhobenen Forderung ein PGP-Server im Staatsministerium für Landesentwicklung und Umweltfragen zur Verfügung. Die flächendeckende Einführung sicherer Verschlüsselungs- und Signaturverfahren im Bayer. Behördennetz ist mit den grundlegenden Beschlüssen und den Anstrengungen bei der Produktauswahl für sichere e-mail zwar einen großen Schritt weiter, aber noch nicht zum Abschluss gekommen. Auch die sichere Abwicklung von Dialogverfahren im Client-Server-Betrieb und von sonstigen Datenübertragungen zwischen Dienststellen darf nicht vergessen werden. Es sind noch große Anstrengungen notwendig, wobei die heterogene technische und personelle Ausstattung der Teilnehmer am Bayer. Behördennetz ein Hemmnis ist, aber auch die Vielzahl der mit diesen Fragen befassten Gremien, von denen keines die Möglichkeit hat, Sicherheitsvorgaben ressortübergreifend festzulegen und durchzusetzen (Nr. 17.1.2).

Die umgehende Sicherstellung einer vertraulichen, authentischen und nicht manipulierbaren Kommunikation im Bayer. Behördennetz ist zwar einige Schritte weitergekommen, aber noch nicht umfassend gewährleistet. Meine entsprechende Forderung ist nach wie vor offen.

Die Anwendung der **Data-Warehouse und Data-Mining** Verfahren ermöglicht es, in unterschiedlichen Datenbeständen bisher unbekannte Zusammenhänge aufzudecken und bisher nicht gestellte Fragen, an die bei der Speicherung der Daten möglicherweise gar nicht gedacht wurde, zu beantworten. Aus Datenschutzsicht muss an das für den Datenschutz zentrale Gebot der Zweckbindung erinnert werden - jeder soll u.a. wissen, zu welchem Zweck seine Daten verarbeitet werden -. Mit diesem Zweckbindungsgebot ist eine Speicherung von personenbezogenen Daten für unbestimmte Zwecke in einem Data-Warehouse nicht vereinbar. In einer Entschließung der Datenschutzkonferenz werden die Hersteller und Anwender deshalb u.a. aufgefordert, durch Anonymisierung oder Pseudonymisierung die Verletzung des Zweckbindungsprinzips zu vermeiden oder jedenfalls eine freie, spezifizierte und jederzeit widerrufliche Einwilligung des

Betroffenen einzuholen (Nr. 17.1.3).

Eine Arbeitsgruppe des AK Technik der Datenschutzkonferenz hat unter meiner Federführung an der Entwicklung von **Schutzprofilen** ("Protection Profiles") gearbeitet, mit denen zur Umsetzung der auf internationaler Ebene vereinbarten **„Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik - Common Criteria Version 2.0 (CC)“** beigetragen werden soll.

Mit diesen Schutzprofilen werden unter anderem auch datenschutzrechtliche Anforderungen für bestimmte Produkttypen definiert, die von den Anwendern gegenüber den Herstellern und Zertifizierungsstellen geltend gemacht werden können. Mit ihnen können international vergleichbare Vorgaben für die Entwicklung datenschutzfreundlicher Produkte erstellt werden, z.B. für die zugriffssichere Speicherung, die gesicherte und vertrauliche Datenübertragung in Netzwerken und für die datenschutzgerechte Erzeugung von Pseudonymen (Nr. 17.1.4).

Ich bewerte diese Arbeit, die noch nicht abgeschlossen ist, deshalb als ausserordentlich wichtig.

Besonders hinweisen will ich auf den Beitrag **„Viren im Internet“** (Nr. 17.1.5), der unter dem Eindruck des Auftretens jüngster Viren (z.B. „I Love You“) Abwehrmaßnahmen gegen verschiedenartige Viren beschreibt. Wegen des nicht ausschließbaren Restrisikos muss der Anschluss sensibler Datenbestände an offene Netze, insbesondere an das Internet, auch bei Einhaltung von Sicherheitsmaßnahmen sorgfältig abgewogen werden.

Aus dem **Komplex Prüfungen** sind zwei Fälle hervorzuheben, die jeweils zu Beanstandungen geführt haben:

In einem Fall stellte eine Universitätsklinik ungenügend anonymisierte Patientendaten ins Netz, um ein spezielles Informationssystem der Klinik vorzustellen. Mit wenigen Schritten konnten sogar die Klarnamen der Patienten offen gelegt werden (Nr. 17.2.1). Das Beispiel zeigt, wie sorgfältig mit der Informationsgestaltung im Internet umgegangen werden muss.

In einem zweiten Fall mussten ebenfalls bei einer Universitätsklinik die nicht ausreichende Si-

cherung von Zimmern, in denen sensible Patientenakten gelagert waren, sowie die nicht sorgfältige Verwaltung von Zimmerschlüsseln gerügt werden. Diese Mängel haben zu einem zeitweiligen Verschwinden zahlreicher, in einem Fall zu einem dauernden Verschwinden von Patientenakten geführt (Nr. 17.2.1).

Im Übrigen habe ich bei einigen Dienststellen nahezu vorbildliche Sicherheitsmaßnahmen festgestellt.

An Mängeln anderwärts nenne ich die Themen u.a. mangelnde Verschlüsselung, mangelhafte Transparenz der Datenverarbeitung und ungenügend ausgebildetes und häufig zu wenig vorhandenes EDV-Personal.

Wesentlicher Schwerpunkt war wieder die **Beratung** zahlreicher Dienststellen zu Fragen der Sicherheit, die mit der zunehmenden Vernetzung der Dienststellen und dem immer größer werdenden Anteil der Datenverarbeitung in der öffentlichen Verwaltung immer größeren Umfang annimmt. Ich weise in diesem Zusammenhang auch auf das Angebot an Orientierungshilfen zu zahlreichen technischen und organisatorischen Fragen auf meiner Website hin (www.datenschutz-bayern.de/inhalte/technik.htm).

Die sachgerechte Erfüllung insbesondere auch der Beratungsaufgaben, an der hohes Interesse der Dienststellen besteht, stellt an das Personal meiner Geschäftsstelle, das im technischen Bereich seit 1983 nicht verstärkt wurde, immer höhere Aufgaben sowohl in quantitativer, aber auch in qualitativer Hinsicht. Eine Verbesserung der personellen Ausstattung meiner Dienststelle im technischen Bereich ist deshalb dringend erforderlich.

1.2.8 Jugendhilfe- und Sozialbereich

Im Jugendhilfe- und Sozialbereich haben mich neben Einzelfragen aus den Bereichen gesetzliche Krankenversicherung, Sozialhilfewesen, Unfall- und Rentenversicherung u.a. die Datenschutzfragen im Zusammenhang mit dem türkischen Jugendlichen „Mehmet“ beschäftigt. Daneben hatte ich mich, auch als Vorsitzender des Arbeitskreises Gesundheit und Soziales der Datenschutzkonferenz, mit der Datenverarbeitung nach dem Gesetzentwurf für eine „Gesundheitsreform 2000“ zu befassen. Schließlich ist eine Prüfung der Kassenärztlichen Vereinigung Bayerns besonders zu erwähnen.

Die Prüfung der **Datenverarbeitung im Fall des türkischen Jugendlichen „Mehmet“** ergab eine Beanstandung der Staatsministerien für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit und des Innern wegen unzulässiger **Datenübermittlung** von besonders geschützten Daten letztlich **an das Kreisverwaltungsreferat** der Landeshauptstadt München. Daneben ergab sich, dass durch das Staatsministerium für Arbeit und Sozialordnung, Familien, Frauen und Gesundheit Daten erhoben wurden, für die mangels Zuständigkeit des Staatsministeriums für die kommunale Rechtsaufsicht und auch mangels des Vorliegens eines rechtsaufsichtlichen Verfahrens keine Datenerhebungsbefugnis vorlag. Ich habe diesen Fall zum Anlass genommen, auf die unglückliche Lage hinzuweisen, wonach das Staatsministerium als fachlich zuständiges Ministerium keine klare Datenerhebungsbefugnis hat. Im Zuge des Dritten Verwaltungsreformgesetzes soll nun mit einer Ergänzung des Gesetzes zur Ausführung des Sozialgesetzbuches Abhilfe geschaffen werden. Das Staatsministerium des Innern hat gegen die Beanstandung remonstriert mit der Begründung, die Datenübermittlung sei erforderlich gewesen. Ich konnte mich dem nicht anschließen und habe die Beanstandung aufrechterhalten (Nr. 4.6.1).

Ebenfalls Gegenstand einer umfangreicheren Prüfung war die **Pressepolitik des Kreisverwaltungsreferats** der Landeshauptstadt München im nämlichen Fall. Hier ergab die Prüfung, dass zu viele, teilweise sensible Daten aus dem Vorleben von „Mehmet“ der Presse übermittelt wurden (Nr. 16.1). Von einer Beanstandung der Landeshauptstadt München habe ich abgesehen, da es sich um eine ausgesprochene Einzelaktion des Kreisverwaltungsreferates gehandelt hatte.

Zum Entwurf eines **Gesundheitsreformgesetzes 2000** habe ich mich in der Sachverständigenanhörung in dem zuständigen Ausschuss des deutschen Bundestages geäussert. Weiter fasste die Datenschutzkonferenz auf Vorschlag des unter meiner Federführung tagenden AK Gesundheit und Soziales eine Entschließung gegen die in dem Entwurf ursprünglich vorgesehene personenbezogene Übermittlung von Patientendaten an die Krankenkassen, was dort den „gläsernen Patienten“ zur Folge gehabt hätte. Statt dessen wurde dann ein Pseudonymisierungsverfahren vorgesehen. Wegen anderer Streitpunkte wurde auch dieser Teil aus dem Entwurf gestrichen, um ein Vermittlungsverfahren zu vermeiden. Es steht zu hoffen, dass diese Gedanken in einer anstehenden Neuregelung der Datenverarbeitung im Gesundheitswesen wieder aufgegriffen werden (Nr. 4.2.1).

Zu beanstanden war die **Kassenärztliche Vereinigung Bayerns** wegen der Übermittlung von Einkommensdaten von Ärzten an einen im Rahmen eines Prüfungsverfahrens als Sachverständigen beauftragten anderen Arzt, der zu den vorgenannten in einem Konkurrenzverhältnis stand. Die Übermittlung war nicht erforderlich, weil die genannten Ärzte nicht Gegenstand des Prüfungsverfahrens waren. Die Frage, ob ein Konkurrent als Sachverständiger beauftragt werden durfte, war von mir nicht zu prüfen, da es sich insoweit nicht um eine datenschutzrechtliche Frage gehandelt hat (Nr. 4.4.1).

1.2.9 Steuer und Statistik

Im Bereich Steuer und Statistik waren neben zahlreichen Einzelfragen auch einige Grundsatzfragen zu behandeln. Hier hervorzuheben sind:

Die Frage, ob die **Schutzvorschriften der Landesdatenschutzgesetze, insbesondere die Auskunfts- und Aufbewahrungsvorschriften, auch auf das Besteuerungsverfahren anzuwenden sind**, wird von der Finanzverwaltung meiner Ansicht nach zu Unrecht verneint. Die AO enthält insoweit keine spezielleren Vorschriften, die Datenschutzgesetze sind die späteren Gesetze. Für die Meinung, der Gesetzgeber habe das Besteuerungsverfahren als, abgesehen vom Steuergeheimnis, datenschutzfreien Raum gewollt, bieten sich keine Anhaltspunkte. Abgesehen davon scheint es höchst zweifelhaft, ob diese Auffassung mit dem verfassungsrechtlichen Rang des

Rechtes auf informationelle Selbstbestimmung vereinbar wäre (Nr. 11.1).

Bei der **Führung von Fahrtenbüchern** für Ärzte kann ein Erfolg vermeldet werden. Der Bundesfinanzminister hat auf Drängen der Datenschutzbeauftragten in einem Schreiben an den Bundesbeauftragten für den Datenschutz als Regelung angekündigt, daß als Grund der Fahrt lediglich „Patientenbesuch“ anzugeben sei und Name und Anschrift des Patienten in einer gesonderten Aufzeichnung niederzulegen seien, die nur bei tatsächlichen Anhaltspunkten für Steuerverkürzung vorzulegen sein sollte. Dagegen hatten die AO-Referenten mehrheitlich „beschlossen“, die unveränderte Führung des Fahrtenbuches zu verlangen. Das Bayerische Finanzministerium hat auf meine eindringlichen Hinweise inzwischen mitgeteilt, dass es sich der Haltung des BMF anschließen werde (Nr. 11.6).

Zur **Vorbereitung des registergestützten Zensus** arbeitet der Bundesminister des Innern an einem **„Zensus-Test-Gesetz“.** Ich habe dazu datenschutzrechtliche Forderungen erhoben, denen sich das Staatsministerium des Innern angeschlossen hat. U.a. habe ich gefordert, die geplante Mehrfachfallprüfung, die beim Statistischen Bundesamt ein bundesweites zentrales Melderegister entstehen ließe, zu überdenken und durch Klarstellungen einen eventuellen Rückfluss von Statistikdaten in den Verwaltungsvollzug zuverlässig auszuschließen (Nr. 14.1).

1.3 Nationale und internationale Konferenzen

Ich nahm in den Berichtsjahren 1999 und 2000 wiederum an den halbjährlich stattfindenden Konferenzen der Datenschutzbeauftragten des Bundes und der Länder teil, die 1999 unter der Federführung meines Kollegen Dr. Kessel, Mecklenburg-Vorpommern und 2000 unter der meines Kollegen Burckhard Nedden, Niedersachsen stattfanden. Die Zusammenarbeit ist wie immer gut und effektiv.

Die Konferenzen befassten sich mit aktuellen Themen von u.a. der Modernisierung des Datenschutzrechts, der Überwachung der Telekommunikation, Fragen von datenschutzfreundlichen Technologien, der Schriftgutaufbewahrung bei Gerichtsbarkeit und Staatsanwaltschaft, der Kryptopolitik, der Gesundheitsreform 2000, von DNA - Analysen auf Grund von Einwilligungen, dem Urteil des Bundesverfassungsgerichts zu den Abhörmaßnahmen des BND, dem Thema Data-Warehouse und Data-Mining, dem polizeilichen Verbunddateisystem „Inpol-neu“ und zur Auftragsdatenverarbeitung durch das BKA für Länderdateien, zum wiederholten Male mit dem Strafverfahrensänderungsgesetz, der Videoüberwachung, den datenschutzrechtlichen Konsequenzen aus der Entschlüsselung des menschlichen Genoms, der serviceorientierten Verwaltung über das Internet bis hin zur der Datensparsamkeit bei der Rundfunkfinanzierung.

Die Entschließungen (siehe Anlagen) habe ich jeweils den zuständigen Ressorts zugeleitet.

Weiter nahm ich 1999 an der internationalen Datenschutzkonferenz teil, die in diesem Jahr in Hongkong statt fand (Flug kaum teurer als nach Kopenhagen, Hotelkosten billiger). Die Konferenz befasste sich mit einer Fülle von Themen grenzüberschreitender Bedeutung, von denen ich hier nur einige nennen kann, wie biometrische Verfahren und Datenschutz, Datenschutzanforderungen in einem global tätigen Unternehmen, Verfolgen von Datenspuren im Internet, elektronische Überwachung der Telekommunikation, internationale polizeilichen Zusammenarbeit im Verhältnis zum Schutz der Privatheit. Weiter habe ich 1999 an der europäischen Datenschutzkonferenz in Helsinki teilgenommen, bei der ein wesentliches Thema die Einrichtung einer Gendatenbank über die isländische Bevölkerung war. Ich habe auf dieser Konferenz über das Neugeborenen-Screening in Bayern berichtet. Einer meiner Mitarbeiter nahm an der Europäischen

Datenschutzkonferenz 2000 in Stockholm teil, Themen waren u.a. der Verfahrensstand in den Europäischen Ländern hinsichtlich der Umsetzung der EG Datenschutzrichtlinie, die Zusammenarbeit in der Bekämpfung der Internet-Kriminalität und die Videoüberwachung in den einzelnen Ländern. Weiter wurde über eine Kontrolle von Gendatenbanken durch die schwedische Datenschutzbehörde berichtet.

1.4 Fazit

Der vorstehende Überblick gibt einen Querschnitt durch unsere Tätigkeit wieder und hebt naturgemäß die aus meiner Sicht bemerkenswertesten Feststellungen hervor. Er soll aber nicht zum Schluss verleiten, dass sich unsere Tätigkeit auf nachträgliche Kritik und das Aufgreifen von Missständen beschränkt. Ein großer Teil unserer Arbeit besteht aus aktueller Beratung von Dienststellen, die sich mit datenschutzrechtlichen Fragen aus ihrem Geschäftsbereich an uns wenden. Meine Mitarbeiter und ich legen großen Wert auf diese Beratung, weil sich dadurch Missstände und Fehler vermeiden lassen. Der Bericht soll auch nicht zu dem Fehlschluss verleiten, dass der Datenschutz in Bayern generell in grobem Maß missachtet wird. Es wird sich zu einem guten Teil um Einzelfeststellungen handeln, die nicht zu verallgemeinern sind. Bei meinen Kontrollen habe ich neben Kritikpunkten vielfach auch eine ordentliche und sorgfältige Beachtung der datenschutzrechtlichen Normen und Grundsätze feststellen können. Der Bericht zeigt Licht und Schatten - wie die vorhergehenden Berichte auch. Positiv im Vergleich zu den Feststellungen im letzten Tätigkeitsbericht möchte ich besonders hervorheben die Fortschritte in der Frage der Speicherungen im Kriminalaktennachweis der Polizei. Jetzt kommt es auf die effektive Umsetzung in den Richtlinien und darauf an, dass die Polizei von den Staatsanwaltschaften die notwendigen Informationen bekommt, um unberechtigte Speicherungen zu löschen. Ich hoffe, ich kann alsbald einen positiven Abschluss dieses Problemkreises berichten.

Ich darf den 19. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz hiermit der Aufmerksamkeit von Landtag und Staatsregierung und nicht zuletzt der Öffentlichkeit empfehlen.

2 Allgemeines Datenschutzrecht

2.1 Datenschutzrecht in der Europäischen Union

2.1.1 Europäische Grundrechte-Charta

Bereits im 18. Tätigkeitsbericht (Nr. 2.1) habe ich auf die Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995 hingewiesen, nach der anlässlich der Überarbeitung der Unions- und Gemeinschaftsverträge ein einklagbares europäisches Grundrecht auf Datenschutz in einen verbindlichen Grundrechtskatalog aufgenommen werden sollte. Der Europäische Rat hat am 04. Juni 1999 in Köln die Einsetzung eines Gremiums beschlossen, das eine Charta der Grundrechte der Europäischen Union erarbeiten sollte. Dieser „Konvent“ - unter dem Vorsitz des ehemaligen Bundespräsidenten Roman Herzog - hat seinen Entwurf einer Grundrechte-Charta am 02. Oktober 2000 dem Europäischen Rat zugeleitet. Angestrebt ist die Grundrechte-Charta im Dezember 2000 bei der EU-Regierungskonferenz in Nizza feierlich zu proklamieren und danach zu prüfen, ob und gegebenenfalls auf welche Weise die Charta in die EG-Verträge aufgenommen werden könnte.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 07./08. Oktober 1999 (vgl. Anlage 11) im Hinblick auf die Verfassungen einiger europäischer Staaten und deutscher Länder sowie die Rechtsprechung des Bundesverfassungsgerichts die Bundesregierung, den Bundestag und den Bundesrat aufgefordert, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Gemeinschaft einzusetzen.

Der Bundesbeauftragte für den Datenschutz hat hierzu in der Anhörung der Europaausschüsse des Bundestages und des Bundesrates „Charta der Grundrechte der Europäischen Union“ am 05. April 2000 für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Stellung genommen. Er hat sich dafür ausgesprochen, einer Formulierung des Datenschutzgrundrechts als Selbstbestimmungsrecht, das heißt als Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und die Verwendung seiner persönlichen Daten zu bestimmen, den Vorzug zu geben. Er hat ferner angeregt, das Datenschutzgrundrecht um das Auskunftsrecht des Betroffenen,

die unabhängige Kontrolle durch den europäischen Datenschutzbeauftragten und das Recht darauf, diesen anrufen zu können, zu ergänzen.

Der der Regierungskonferenz vorgelegte Entwurf der Grundrechte-Charta (Charte 4487/00 vom 28. September 2000) enthält in Art. 8 ein Datenschutzgrundrecht als Recht einer Person auf den Schutz ihrer personenbezogenen Daten. Danach dürfen diese Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung des Betroffenen oder aufgrund einer sonstigen gesetzlichen Grundlage verarbeitet werden. Weiterhin soll jede Person das Recht auf Auskunft und Berichtigung erhalten und die Überwachung der Einhaltung dieser Vorschriften durch eine unabhängige Stelle gewährleistet sein.

2.1.2 Datenschutzvorschriften für die Verwaltungsbehörden der EU

Ferner habe ich in meinem 18. Tätigkeitsbericht ausgeführt, dass eine Umsetzung der EG-Datenschutzrichtlinie vom 24. Oktober 1995 in verbindliche Datenschutzvorschriften für die Verwaltungsbehörden der EU noch aussteht, obwohl die Richtlinie seit 01. Januar 1999 auch auf die Einrichtungen und Organe der EU anwendbar ist. Die Europäische Kommission hat im Berichtszeitraum einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vorgelegt. Der Verordnungsvorschlag lehnt sich in weiten Teilen an die EG-Datenschutzrichtlinie von 1995 an. Für besonders wichtig halte ich die Einrichtung einer Kontrollbehörde, des europäischen Datenschutzbeauftragten, der für die Überwachung der Anwendung der Bestimmungen der Verordnung und aller anderen Rechtsakte der Gemeinschaft zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch ein Organ oder eine Einrichtung der Gemeinschaft verantwortlich ist. Er soll die ihm zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Ich hoffe, dass diese Vorschriften in absehbarer Zeit in Kraft treten werden.

2.2 Umsetzung der EG-Datenschutzrichtlinie

2.2.1 Novellierung des BDSG

In einer Entschließung ihrer 57. Konferenz am 25./26. März 1999 haben die Datenschutzbeauftragten des Bundes und der Länder gefordert, die notwendige umfassende Novellierung des BDSG nicht länger aufzuschieben (vgl. Anlage 3). Inzwischen liegt ein vom Bundeskabinett am 14. Juni 2000 beschlossener Gesetzentwurf zur Novellierung des BDSG vor.

Er enthält zwar im Gegensatz zu den Vorentwürfen einige der innovativen Elemente, die ich im 18. Tätigkeitsbericht (Nr. 2.2.1) gefordert habe. So ist eine Regelung zu den Grundsätzen der Datenvermeidung und der Datensparsamkeit enthalten, an denen sich die Gestaltung und die Auswahl von Datenverarbeitungssystemen auszurichten haben. Ferner wurde der Vorrang anonymer und pseudonymer Formen der Datenverarbeitung – als Ausprägung des Grundsatzes der Erforderlichkeit – ausdrücklich aufgenommen. Es finden sich außerdem Regelungen zur Zulässigkeit der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) und zum Datenschutzaudit, das das Ziel verfolgt, datenschutzgerechte Produkte zu fördern. Eine Chipkartenregelung ist leider – anders als in einem Vorentwurf – nicht mehr enthalten.

Von einer näheren inhaltlichen Bewertung sehe ich im Hinblick auf die Zuständigkeit des Bundesbeauftragten für den Datenschutz ab.

Die Fraktionen der Regierungskoalition haben sich darauf verständigt, in einer „Zweiten Stufe“ der Novellierung des BDSG eine grundlegende Modernisierung des Datenschutzrechts in Deutschland zu initiieren. Hierzu hat im Juni 2000 in Berlin eine Auftaktveranstaltung mit dem Thema „Modernisierung des Datenschutzrechts“ stattgefunden. Experten aus den Bereichen Recht und Informatik sollen zudem Gutachten über die juristischen und technischen Aspekte einer grundlegenden Modernisierung des Datenschutzrechts vorlegen. Das gesamte Projekt soll von einem Beirat mit Mitgliedern aus Wissenschaft, Wirtschaft, Verwaltung und weiteren Datenschutzexperten begleitet werden, der die Arbeit der Gutachter bewertet und weitere Überlegungen einbringt. Ferner sind kleinere Expertengruppen („Satelliten“) vorgesehen, die bestimmte

abgegrenzte Themenbereiche bearbeiten. Auf diesem Weg soll die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an diesen Arbeiten beteiligt werden. Es ist beabsichtigt, die auf diesen Grundlagen erarbeiteten Entwürfe der Bundesregierung nicht nur im Kreis der Ausschüsse und innerhalb des Beirats zu diskutieren, sondern auch im Internet zur Diskussion zu stellen. Dies wird auch als wichtiger Versuch angesehen, erstmals in Deutschland weitergehende Schritte in den Bereich der „eDemocracy“ zu gehen.

Ich hoffe, dass in dieser „Zweiten Stufe“ die längst überfällige Modernisierung des Datenschutzrechts in Deutschland erreicht werden kann. Insbesondere von der Beteiligung der Öffentlichkeit an dem Diskussionsprozess verspreche ich mir eine bessere Verständlichkeit des Gesetzes und ein stärkeres Eingehen auf aktuelle Entwicklungen. Ich werde auch selbst an dieser Diskussion teilnehmen.

2.2.2 Novellierung des BayDSG

Die aufgrund der Vorgaben der EG-Datenschutzrichtlinie bis zum 24. Oktober 1998 (vgl. 18. Tätigkeitsbericht, Nr. 2.2) zu novellierenden Bestimmungen des Bayerischen Datenschutzgesetzes (BayDSG) sind zu ihrem größten Teil zum 01. Dezember 2000 geändert worden. Zwar war der bayerische Gesetzgeber damit etwas schneller als der Bundesgesetzgeber. Inhaltlich sind die Änderungen des BayDSG jedoch noch hinter dem Entwurf des BDSG sowie anderen Landesdatenschutzgesetzen zurückgeblieben.

Von den Vorschlägen, die ich während der Konzeptionsphase des Entwurfs durch das federführende Staatsministerium des Innern einbringen konnte, wurde leider nur ein Teil übernommen. Besonders erfreulich ist, dass die bloße Anlasskontrolle bei nur in Akten zu verarbeitenden Daten beseitigt wurde und grundsätzlich für alle bayerischen öffentlichen Stellen die Berufung interner Datenschutzbeauftragter gesetzlich vorgeschrieben wurde (vgl. hierzu den 17. Tätigkeitsbericht, Nr. 2.1). Auch ist die Einschränkung meines Kontrollrechts beim Widerspruch Betroffener - wie bei der Regelung im Entwurf des BDSG - nur noch bei der Sicherheitsüberprüfung vorgesehen; allerdings sollte die Möglichkeit des Widerspruchs auch dort gestrichen werden. Schließlich wurden ein Anrufungsrecht der Beschäftigten an den behördlichen Datenschutzbe-

auftragten sowie Vorschriften zu meiner rechtzeitigen Unterrichtung bei Gesetzesvorhaben und zur Erhöhung der Geldbuße bei Datenschutzverstößen in den Gesetzentwurf übernommen. Vor allem aber wurde gesetzlich bestimmt, dass alle öffentlichen Stellen, die automatisierte Verfahren mit personenbezogenen Daten einsetzen, behördliche Datenschutzbeauftragte zu bestellen haben; dies entspricht meiner Forderung im 17. (unter Nr. 2.1) und 18. Tätigkeitsbericht (unter Nr. 2.2.2). Bisher war die Bestellung durch Verwaltungsvorschrift lediglich staatlichen Behörden aufgegeben; für Kommunen bestand nur eine Empfehlung. Das sind immerhin wesentliche Verbesserungen.

Ansonsten läßt das novellierte BayDSG innovative Gesichtspunkte weitgehend vermissen. Zwar habe ich grundsätzlich Verständnis dafür, dass im Hinblick auf die Eilbedürftigkeit der Umsetzung der EG-Datenschutzrichtlinie, wie bei dem Entwurf der Bundesregierung, von einem Zweistufenkonzept ausgegangen wird und einzelne von mir vorgeschlagene Änderungen oder Neuregelungen nicht bereits jetzt, sondern erst in der zweiten Stufe behandelt werden sollen. Ich sehe allerdings auch die Frage, wann diese zweite Stufe realisiert werden wird. Zumindest in dieser zweiten Stufe sollten unter anderem noch folgende Komplexe geregelt werden:

Die Informationsgesellschaft ist durch die immer stärkere Miniaturisierung der Bauelemente von Rechnern, die sich ständig erhöhende Leistung dieser Elemente, durch die Entwicklung immer leistungsfähigerer Software, die Vernetzung der Systeme und durch immer komplexere Datenbanksysteme gekennzeichnet. Damit gehen immer weiter gehendere Möglichkeiten der Verarbeitung personenbezogener Daten einher. Die Forderung des Bundesverfassungsgerichts im Volkszählungsurteil, dass der Einzelne grundsätzlich selbst bestimmen können muss, wer, was, wann über ihn weiß und was er damit für Zwecke verfolgt, ist unter diesen Randbedingungen einer wesentlich höheren Belastung ausgesetzt.

- Erforderlich ist vor diesem Hintergrund eine Regelung zur Datenvermeidung und zur Datensparsamkeit, die ihr Vorbild im Teledienstedatenschutzgesetz und im Mediendienste-Staatsvertrag hat. Diese Regelungen besagen, dass Datenverarbeitungssysteme so einzurichten sind, dass sie mit möglichst wenigen personenbezogenen Daten auskommen. Mit der Aufnahme dieser Grundsätze würde zum einen das Prinzip der Erforderlichkeit verdeutlicht, zum anderen würden die Behörden zu einer sorgfältigen Prüfung angehalten, welches Maß

an Datenverarbeitung zur Aufgabenerledigung unumgänglich ist. Außerdem würde der Charakter des BayDSG als Datenschutzgesetz hervorgehoben. Im Übrigen beziehen sich die Gebote der Datenvermeidung und der Datensparsamkeit vor allem auf die Gestaltung informationstechnischer Systeme. Sie haben damit einen teilweise anderen Regelungsbereich als das Gebot der Erforderlichkeit, das sich auf die einzelne Datenverarbeitung bezieht.

- Erforderlich ist zudem eine Regelung zum Vorrang anonymer und pseudonymer Formen der Datenverarbeitung. Sie ist z. B. im Gesundheitsbereich (etwa für Laboruntersuchungen), aber auch im Forschungsbereich notwendig.

- Ferner halte ich eine Chipkarten-Regelung für notwendig, da durch immer leistungsfähigere Prozessorchips Datenverarbeitungssysteme auf immer kleinerem Raum zur Verfügung stehen. Diese Systeme stellen mobile personenbezogene Speicher- und Verarbeitungsmedien dar, die vom Betroffenen mitgeführt werden und mit anderen elektronischen Geräten kommunizieren können. Sie bringen für den Betroffenen nicht nur Vorteile mit sich, sondern bergen durch mangelnde Transparenz, die mögliche Konzentration von Daten und Datenverarbeitungen aus den verschiedenen Lebensbereichen und Behördenzuständigkeiten und schließlich durch die mögliche mangelnde Sicherheit spezifische Gefahren für das Recht der Menschen auf informationelle Selbstbestimmung. In das BayDSG sollte deshalb eine Bestimmung über mobile Speicher- und Prozessorsysteme aufgenommen werden, die unter anderem Aussagen über die Frage der datenverarbeitenden Stelle, die Notwendigkeit der Vorabkontrolle sowie über die Pflichten der diese Systeme ausgebenden Stellen zur Unterrichtung des Betroffenen enthalten. Deren Unterrichtung über die Einzelheiten der Datenverarbeitung ist notwendig, damit sie für ihn transparent ist und er weiß, in welchen Bahnen der Datenverarbeitungsprozess abläuft, wie er zu beeinflussen ist und wem gegenüber er seine Rechte als Betroffener geltend machen kann.

- Da im öffentlichen Raum zunehmend Videokameras eingesetzt werden, halte ich eine Regelung zur Videoüberwachung auch im BayDSG für notwendig. Der Einsatzbereich dieser Kameras geht von Verkehrsbeobachtungssystemen, über Videokameras an Bahnanlagen, öffentlichen Gebäuden, Wertstoffhöfen von Gemeinden bis hin zu Beobachtungen von Flächen durch die Polizei, die besonders kriminalitätsbelastet sind oder Schwerpunkte polizeilicher

Gefahren darstellen. Hinzu kommt die Nutzung von Kameras durch die Polizei, die ursprünglich von anderen Bedarfsträgern (z. B. kommunalen Verkehrsbetrieben) zu anderen Zwecken aufgestellt wurden.

Die Tendenz zu einer immer flächenhafteren Beobachtung mit Videokameras ist mit dem gegebenen Rechtsinstrumentarium im allgemeinen Datenschutzrecht und dem bereichsspezifischen Polizeirecht nicht mehr zu bewältigen. Es muss die Entwicklung hin zu einer flächendeckenden Beobachtung des Einzelnen verhindert werden, wobei bereits die bloße Beobachtungsmöglichkeit problematisch ist. Die inzwischen vorhandene und sich immer weiter verbessernde Technik erlaubt es nicht, sich mit der Feststellung zu bescheiden, die bloße Beobachtung von Räumen ohne Aufzeichnung und Heranzoomen von Personen sei als Übersichtsaufnahme kein relevanter Eingriff. Zum einen ist für den Bürger nicht erkennbar, ob gerade aufgezeichnet und/oder gezoomt wird oder nicht, zum anderen ermöglicht es die digitale Bildbearbeitung auch aus Übersichtsaufnahmen erkennbare Personen herauszuarbeiten. Damit verschwimmen die Grenzen zwischen Übersichtsaufnahmen und dem Erheben von personenbezogenen Daten. Deshalb muss bereits das Aufstellen von Beobachtungseinrichtungen selbst gesetzlich geregelt und begrenzt werden. Neben einer bereichsspezifischen Regelung im Polizeirecht ist eine solche wegen der nicht polizeilichen Anwendungen auch im BayDSG notwendig.

Weiterhin sollten die Rechte der betroffenen Bürger und die Transparenz der Datenverarbeitung verbessert werden. Ein wesentlicher Schwerpunkt der EG-Datenschutzrichtlinie ist es, die Rechte der von der Datenverarbeitung betroffenen Bürger durch Auskunfts- und Berichtigungsansprüche, sowie durch eine Beschränkung der Verarbeitung besonders sensibler Daten zu stärken. Gerade die Auskunftsansprüche stellen einen wesentlichen Kern der Realisierung des Rechts auf informationelle Selbstbestimmung dar. Eine Beschränkung dieser Auskunftsansprüche greift in diesen Kern ein. Ich halte daher folgende Regelungen des BayDSG für überdenkenswert:

- Unverhältnismäßig ist die Möglichkeit einer Auskunftsverweigerung der betroffenen Behörde schon zu Zwecken der Verhinderung und Verfolgung bloßer Ordnungswidrigkeiten.

- Die EG-Datenschutzrichtlinie sieht unter anderem vor, dass der Betreffende unter anderem über die Datenempfänger und über Auskunfts- und Berichtigungsrechte Informationen erhält, soweit dies notwendig ist, um „gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten“. Das BayDSG enthält eine derartige Regelung nicht; sie wird nicht für erforderlich gehalten, da bei den an die Gesetze gebundenen öffentlichen Datenverarbeitern sowieso die Verarbeitung „nach Treu und Glauben“ gewährleistet sei. Im Hinblick auf die Bedeutung dieser Auskünfte für die Betroffenen zur Verfolgung ihrer Rechte würde ich gleichwohl eine entsprechende Regelung im BayDSG begrüßen.

- Ferner wird in einer neuen Sonderregelung des BayDSG die an sich vorgesehene grundsätzliche Pflicht zur Benachrichtigung über Datenspeicherungen für Behörden der Staatsanwaltschaft, für Justizvollzugsanstalten, für Führungsaufsichtsstellen und für Stellen der Gerichts- und Bewährungshilfe generell ausgeschlossen. Dieser generelle Ausschluss wird zwar nicht an der in der EG-Datenschutzrichtlinie enthaltenen Benachrichtigungspflicht zu messen sein, da die Richtlinie für Datenspeicherungen der Behörden der Staatsanwaltschaft usw. keine Anwendung findet. Ich halte ihn aber unabhängig von der Richtlinie im Hinblick auf das Prinzip der Erforderlichkeit für zu weitgehend. Ich sehe keinen Grund, warum hinter den Benachrichtigungspflichten, wie sie etwa § 101 Abs. 1 StPO vorsieht, zurückgegangen werden soll.

- Das gleiche gilt für die generelle Freistellung der Staatsanwaltschaften, Justizvollzugsanstalten und Behörden der Finanzverwaltung von der Begründungspflicht einer Auskunftsverweigerung.

Außerdem sehe ich in dem neuen BayDSG zu weitgehende Verarbeitungsmöglichkeiten sensibler Daten:

- Die EG-Datenschutzrichtlinie sieht ein grundsätzliches Verbot der Verarbeitung sensibler Daten vor, lässt dazu aber Ausnahmen aufgrund einer nationalen Rechtsvorschrift unter anderem aus Gründen „eines wichtigen öffentlichen Interesses“ zu. Zwar verstoßen die im BayDSG festgelegten Ausnahmen vom Verbot der Verarbeitung sensibler Daten zur Verhinderung und Verfolgung von Ordnungswidrigkeiten nicht gegen diese Bestimmungen, da die

Richtlinie auf das Gebiet der öffentlichen Sicherheit und der Strafverfolgung überhaupt nicht anwendbar ist. Gleichwohl sollte geprüft werden, ob die Verarbeitung sensibler Daten nicht auch unabhängig von der Richtlinie aus Gründen der Verhältnismäßigkeit auf Sicherheitsstörungen von erheblichen Gewicht beschränkt bzw. bezüglich der Verfolgung von Ordnungswidrigkeiten gestrichen werden sollte.

- Ich halte es aus den gleichen Gründen für zweifelhaft, ob die im BayDSG enthaltene generelle Freistellung von Behörden der Staatsanwaltschaft, der Justizvollzugsanstalten, der Führungsaufsichtsstellen sowie der Stellen für Gerichts- und Bewährungshilfe vom grundsätzlichen Verbot der Verarbeitung sensibler Daten gerechtfertigt ist. Auch die Freistellung dieser Stellen und der Polizei vom grundsätzlichen Verbot einer nachteiligen Entscheidung alleine auf der Grundlage einer automatisierten Verarbeitung zum Zweck der Bewertung einzelner Persönlichkeitsmerkmale halte ich für zu weitgehend.

Neben den oben angesprochenen Gesichtspunkten werde ich zur zweiten Stufe unter anderem noch eine Ersetzung der bisherigen „10 Gebote“ im Bereich technischer und organisatorischer Maßnahmen durch Sicherheitsziele, die Neuabgrenzung meiner Kontrollzuständigkeit gegenüber den Gerichten durch das Abgrenzungskriterium der richterlichen Unabhängigkeit sowie die Einbeziehung des vor der Gnadenentscheidung ablaufenden Gnadenverfahrens in den Geltungsbereich des BayDSG anregen.

Die Staatsregierung hat zu erkennen gegeben, dass sie in der zweiten Stufe zumindest Regelungen zu Chipkarten, zur Videoüberwachung, zur Anonymisierung und Pseudonymisierung sowie eine Neukonzeption der „10 Gebote“ für bedenkenswert hält.

2.3 Datenschutz und Forschung

2.3.1 Grundsätzliche Anforderungen an die datenschutzgerechte Ausgestaltung von Forschungsvorhaben

Immer wieder treten öffentliche Forschungseinrichtungen – z. B. Universitäten und wissenschaftliche Institute – mit Fragen zur datenschutzgerechten Ausgestaltung von Forschungsprojekten an mich heran. Bereits im 15. Tätigkeitsbericht (Nr. 2.2) habe ich zur Forschung mit Patientendaten Stellung genommen. Im 18. Tätigkeitsbericht (Nr. 2.3.1) habe ich die Rahmenbedingungen einer ordnungsgemäßen Verarbeitung von Daten bei medizinischen Forschungsvorhaben dargestellt. Die unabhängig vom Forschungsgebiet wesentlichen Anforderungen an eine datenschutzgerechte Ausgestaltung von Forschungsvorhaben sind folgende:

- Vom Schutz des Persönlichkeitsrechts (Datenschutz) i.S. des Art. 1 BayDSG umfasst sind gemäß Art. 4 Abs. 1 BayDSG nur „personenbezogene“ Daten; dies sind „Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene)“. Auch in der Forschung gilt daher der allgemeine datenschutzrechtliche Grundsatz der Erforderlichkeit und damit der Vorrang der Verarbeitung nicht personenbezogener bzw. nicht personenbeziehbarer Daten. Wissenschaftler müssen sich daher zunächst fragen, ob die Verarbeitung personenbezogener Daten überhaupt erforderlich ist. Falls der Forschungszweck auch ohne personenbezogene Daten erreicht werden kann, muss auf sie verzichtet werden. Sollte die Verarbeitung personenbezogener Daten erforderlich sein, müssen in einem zweiten Schritt die aus fachlicher Sicht erforderlichen Daten festgelegt werden.

- Daten sind nicht personenbezogen im Sinne des Datenschutzrechts, wenn sie anonymisiert oder pseudonymisiert sind. Gemäß Art. 4 Abs. 8 des Bayerischen Datenschutzgesetzes (BayDSG) ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr (= absolute Anonymisierung) oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft (= faktische Anonymisierung) einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

In der Forschung wird häufig zwar keine absolute, i.d.R. jedoch eine faktische Anonymisierung in Betracht kommen. Entscheidend ist dabei, dass der Betroffene für den Adressaten der Daten nicht mehr bestimmbar ist. Dabei kommt es unter anderem auf folgende Gesichtspunkte an:

Zum einen ist bezüglich der Möglichkeit einer Reindividualisierung des Betroffenen der ggf. erforderliche Aufwand an Zeit, Kosten und Arbeitskraft zu berücksichtigen. Zum anderen darf ein möglicherweise vorhandenes Zusatzwissen des Empfängers der Daten nicht außer Acht gelassen werden. Dieses Zusatzwissen kann sich z. B. aus öffentlichen Quellen (Presse, Rundfunk etc.), aber auch aus anderen Datenverarbeitungen (z. B. anderen Forschungsvorhaben) des Empfängers ergeben.

Der bloße Verzicht auf den Vor- und den Nachnamen des Patienten führt in der Regel nicht zu einer Anonymisierung. Zumeist müssen zusätzlich andere personenbezogene Merkmale entfallen. Dies sind z. B. das (genaue) Geburtsdatum, der Wohn- und/oder der Geburtsort einschließlich der (vollständigen) Postleitzahl, die (genaue) Berufsangabe und weitere mehr oder weniger identifizierende Merkmale. Häufig wird es für den Zweck des Forschungsvorhabens genügen, entsprechende Gruppenangaben (Altersgruppe, Region, Berufsgruppe etc.) zu verwenden.
Auch bei ausreichend pseudonymisierten Daten handelt es sich um nicht personenbezogene Daten. Pseudonymisieren ist nach dem Gesetzentwurf zur Novellierung des BDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Für eine aus datenschutzrechtlicher Sicht ausreichende Pseudonymisierung müssen sinngemäß die dargestellten Wirkungen einer (faktischen) Anonymisierung erreicht werden.

- Art. 15 Abs. 1 BayDSG bestimmt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig sind, wenn das BayDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Bereichsspezifische Forschungsregelungen sind z. B. Art. 27 Abs. 4 Sätze 1 bis 3 des Bayerischen Krankenhausgesetzes (BayKrG) und Art. 11 Abs. 1 des Bayerischen Krebsregisterge-

setzes (BayKRG).

Die neue Fassung des BayDSG enthält mit Art. 15 Abs. 7 Nr. 7 eine Vorschrift, die es erlaubt, sensible Daten für Forschungsvorhaben zu erheben, zu verarbeiten oder zu nutzen, wenn es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Diese Vorschrift gibt jedoch keine Befugnis zur Durchbrechung der in § 203 Abs. 1 StGB genannten (Berufs-)Geheimnisse, z. B. der ärztlichen Schweigepflicht (vgl. Art. 2 Abs. 9 BayDSG sowie Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 2 Rn. 87).

- Die Verarbeitung personenbezogener Daten im Rahmen von Forschungsvorhaben ist außerdem aufgrund der freiwilligen und informierten Einwilligung des Betroffenen zulässig. Die rechtlichen Voraussetzungen einer wirksamen Einwilligung regelt Art. 15 Abs. 2 bis 4 BayDSG.

  Eine Einwilligung ist nur wirksam, wenn der Betroffene zur Disposition über die personenbezogenen Daten befugt ist. Dies wird bezüglich seiner Daten in der Regel der Fall sein. Außerdem muss er einwilligungsfähig sein. Dieser Gesichtspunkt ist besonders bei Kindern und Jugendlichen, sowie bei nicht einwilligungsfähigen Erwachsenen zu beachten. In diesen Fällen ist dann ggf. die Einwilligung des – hierzu ermächtigten – gesetzlichen Vertreters einzuholen, die ebenfalls allen Anforderungen an eine wirksame Einwilligung genügen muss. Falls die gesetzlichen Vertreter einwilligen, besteht für den Betroffenen jedoch kein Zwang zur Teilnahme an dem Forschungsvorhaben. Bei älteren Jugendlichen (ab etwa 15 Jahre) und beschränkt Einwilligungsfähigen, die (bereits) die entsprechende Einsichtsfähigkeit besitzen, bedarf es deren Einwilligung. Sollten daneben personenbezogene Daten Dritter, z. B. aus dem familiären und sozialen Umfeld erhoben werden, ist auch die Einwilligung der dadurch Betroffenen einzuholen.

  Die Freiwilligkeit der Einwilligung setzt voraus, dass weder ein tatsächlicher noch ein fakti-

scher Zwang auf den Betroffenen ausgeübt wird. Er ist darauf hinzuweisen, dass ihm aus einer Nichtteilnahme keine Nachteile erwachsen.

Außerdem muss der Betroffene die Bedeutung und die Tragweite seiner Einwilligung überblicken können. Die notwendige Informiertheit der Einwilligung verlangt daher unter anderem eine vorherige Unterrichtung des Betroffenen über die Modalitäten der Datenverarbeitung, über den Empfänger der personenbezogenen Daten und über die technisch-organisatorischen Sicherheitsmaßnahmen.

Außerdem bedarf die Einwilligung gemäß Art. 15 Abs. 3 Satz 1 BayDSG der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Im Bereich der wissenschaftlichen Forschung liegen solche besonderen Umstände auch dann vor, wenn der bestimmte Forschungszweck durch die Schriftform erheblich beeinträchtigt würde, Art. 15 Abs. 3 Satz 2 BayDSG. Als Beispiele wären hier Telefonumfragen und Umfragen bei Personengruppen, die gegen schriftliche Erklärungen Mißtrauen hegen, zu nennen; bei telefonischen Umfragen empfehle ich allerdings regelmäßig eine schriftliche Vorinformation, da hiermit die Überrumpelung der Teilnehmer vermieden und die Akzeptanz des Vorhabens gesteigert werden kann (vgl. auch den 18. TB, Nr. 3.1.2). Alleine die Furcht vor einer höheren Ablehnungsquote bei der Datenerhebung kann keinesfalls als relevante Beeinträchtigung des Forschungszwecks angesehen werden. Sinn der Schriftform ist es gerade, dazu beizutragen, dass sich der Betroffene seine Entscheidung, ob er an einem Forschungsvorhaben teilnehmen will, gut überlegt. Wenn sich aufgrund dieser Überlegung eine höhere Ablehnungsquote ergibt, muss dies hingenommen werden. Wenn von der Schriftform abgewichen werden kann, sind die Hinweise an den Betroffenen (Art. 15 Abs. 2 BayDSG) und die Gründe, aus denen sich die erhebliche Beeinträchtigung des wissenschaftlichen Forschungszwecks ergibt, schriftlich festzuhalten, Art. 15 Abs. 3 Satz 3 BayDSG.

- Bei der Einwilligungserklärung ist auch zu beachten, dass eine zu weitgefasste und damit zu unbestimmte Formulierung als Einwilligung auf Vorrat unzulässig ist, weil für den Einwilligenden nicht hinreichend absehbar ist, wofür er seine Einwilligung erteilt. Auch wenn ein Betroffener in die Verarbeitung seiner personenbezogenen Daten einwilligt, gilt der Grund-

satz der Erforderlichkeit.

- Gemäß Art. 17 Abs. 1 Nr. 2 BayDSG ist das Speichern, Verändern oder Nutzen personenbezogender Daten grundsätzlich nur zulässig, wenn es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Abweichend davon ist das Speichern, Verändern oder Nutzen personenbezogener Daten für andere Zwecke (Zweckänderung) u.a. gemäß Art. 17 Abs. 2 Nr. 11 BayDSG dann zulässig, wenn es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Art. 17 Abs. 2 Nr. 11 BayDSG stellt eine Ausnahme von der Zweckbindung des allgemeinen Datenschutzrechts dar, erlaubt hingegen keine Durchbrechung der ärztlichen Schweigepflicht. Eine Ausnahme von der ärztlichen Schweigepflicht bedürfte der Einwilligung des Patienten, soweit keine bereichsspezifische Befugnis zur Datenübermittlung vorliegt. In diesem Fall wäre es grundsätzlich möglich, die Formulierung der Einwilligungserklärung weiter zu fassen, wobei sie in jedem Fall auch den ursprünglichen Forschungszweck umfassen muss. Erhebliche Abweichungen von diesem können mit einer zu weitgefassten Einwilligung nicht gerechtfertigt werden. Zulässig wäre es auch, nachträglich eine neue Einwilligung einzuholen (vgl. auch den 18. TB, Nr. 2.3.1).

- Weiterhin ist auf die Anforderungen des Art. 23 BayDSG zur Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen hinzuweisen.

- Der interne Datenschutzbeauftragte (Art. 25 Abs. 2 bis 4 BayDSG n.F.) sollte frühzeitig in die Planung des Forschungsvorhabens einbezogen werden, wenn die Verarbeitung personenbezogener Daten beabsichtigt ist. In datenschutzrechtlichen Zweifelsfällen – die dezidiert darzulegen und rechtlich zu bewerten sind – kann sich dieser unmittelbar an mich wenden (Art. 25 Abs. 3 S. 3 BayDSG n.F.).

2.3.2 Forschungsvorhaben

2.3.2.1 PISA-Schulleistungsstudie der OECD

Die internationale Schulleistungsstudie PISA (Programme for International Student Assessment) ist Teil des Indikatorenprogramms INES (Indicators of Educational Systems) der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). Ziel dieses Programms ist es, den OECD-Mitgliedsstaaten vergleichende Daten über die Leistungsfähigkeit ihrer Bildungssysteme zur Verfügung zu stellen. Hierzu soll die Studie in den Jahren 2000, 2003 und 2006 in 32 Industriestaaten Leistungen von 15-jährigen Schülern in den Bereichen Leseverständnis, Mathematik und Naturwissenschaften messen. Ferner sollen fächerübergreifende Kompetenzen erfasst werden, die für methodisches Vorgehen, selbstständiges Lernen und kooperatives Arbeiten notwendig sind. Diese Ergebnisse sollen unter Berücksichtigung sozialer Lern- und Lebensbedingungen der Schüler ausgewertet werden.

Die Länder Deutschlands beteiligen sich an der Studie gemäß einer Vereinbarung zwischen dem Bundesministerium für Bildung und Forschung und der ständigen Konferenz der Kultusminister der Länder. Im Jahr 1999 wurde zunächst ein so genannter „Feldtest“ durchgeführt, der der Vorauswahl der zu befragenden 15-jährigen Schüler, der Verteilung der umfangreichen Fragebögen und der Ermittlung der Schülerteilnahme an den Leistungstests diente. Verantwortlich für die Durchführung der Studie ist ein nationales Konsortium mehrerer Universitäten und Forschungseinrichtungen unter der Federführung des Max-Planck-Instituts für Bildungsforschung (MPI) in Berlin. Die Feldarbeit und die Datenverarbeitung hat das so genannte Data Processing Center der International Association for the Evaluation of Educational Achievement (IEA-DPC) in Hamburg übernommen.

Leider wurden ich und auch die meisten anderen Landesdatenschutzbeauftragten erst sehr spät von dem Feldtest und der Studie informiert. Der Hessische Landesbeauftragte für den Datenschutz hat als Vorsitzender des Arbeitskreises Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder die Stellungnahmen der Datenschutzbeauftragten koordiniert und dem MPI die datenschutzrechtlichen Anforderungen an die Studie mitgeteilt. Trotz des Zeitdrucks konnten wichtige Verbesserungen erreicht werden:

- Ich habe darauf hingewiesen, dass die Studie, weil es keine Rechtsgrundlage für die Datenerhebung (z. B. im BayEUG) gibt, eine informierte und freiwillige Einwilligung der Betroffenen voraussetzt. Dies gilt sowohl hinsichtlich der beteiligten Schüler als auch bezüglich ihrer Eltern.

  Die zunächst vorgelegten Informationsschreiben für die Eltern und die teilnehmenden Schüler genügten nicht den Anforderungen an eine ausreichende Information, die datenschutzrechtliche Voraussetzung für die Wirksamkeit einer Einwilligung ist. Ich habe darauf hingewiesen, dass sich aus den Informationsschreiben zumindest stichpunktartig die Art der zu erhebenden Daten ergeben muss. Dies war hier auch deshalb notwendig, weil die Erhebungsbögen z. B. auch Fragen zum persönlichen Umfeld der Schüler und zum Erziehungsverhalten der Eltern enthalten, mit denen nicht ohne weiteres gerechnet werden musste. Außerdem enthält die Elterninformation nunmehr einen Hinweis darauf, dass die Möglichkeit besteht, die vollständigen Fragebögen an den Schulen einzusehen.

  Ferner wurde in das Informationsschreiben für die Eltern ein deutlicher Hinweis darauf aufgenommen, dass die Einwilligung freiwillig ist und sich aus einer Nichtteilnahme keine Nachteile für den Schüler ergeben. Die Schüler wurden darauf hingewiesen, dass ihnen, auch bei Einwilligung ihrer Eltern, die Teilnahme an der Befragung freistehe.

- Außerdem sollten in die vom IEA-DPC den Schulen zur Verfügung gestellten Schülerlisten, anhand derer die Schüler ermittelt wurden, sowie in die Fragebogen für die Schüler die genauen Geburtsdaten der Schüler eingetragen werden. Um eine ausreichende Anonymisierung zu erreichen, wurde dieses Datum gestrichen.

- Die Projektkoordinatoren der Studie haben moniert, dass der Rücklauf unterschriebener Einverständniserklärungen der Eltern von Berufsschülern gering gewesen sei. Dies sei darauf zurückzuführen, dass es viele Schüler versäumt hätten, die Einverständniserklärungen zu Hause abzugeben und am nächsten Schultag wieder zur Schule mitzubringen. Die Koordinatoren schlugen daher vor, in Berufsschulen aktive Elterngenehmigungen durch „passive“ Genehmigungen zu ersetzen. Anstatt schriftliche Einverständniserklärungen einzuholen, sollte den Eltern Gelegenheit gegeben werden, gegen die Teilnahme ihrer Kindes Wider-

spruch einzulegen.

Ich habe darauf hingewiesen, dass eine Verwendung so genannter „passiver“ Elterneinwilligungen in beruflichen Schulen mit dem Bayerischen Datenschutzgesetz nicht vereinbar ist. Gemäß Art. 15 Abs. 1 BayDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das BayDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Erforderlich ist also auch hier die ausdrückliche, freiwillige und informierte Einwilligung. Die angedachte Widerspruchslösung hätte das Regel-Ausnahmeverhältnis bei der Verarbeitung personenbezogener Daten (Regel ist das Verbot der Verarbeitung personenbezogener Daten, die Zulässigkeit der Datenverarbeitung ist die Ausnahme) in sein Gegenteil verkehrt.

2.3.2.2 IEA-Studie Civic Education

Wie die PISA-Studie wird auch die IEA-Studie Civic Education vom Max-Planck-Institut für Bildungsforschung in Berlin durchgeführt. Hierbei handelt es sich um eine internationale Studie zur politischen Bildung von Schülern der 8. Jahrgangsstufe, an der 27 Staaten teilnehmen. Dabei haben die Schüler einen umfangreichen Fragebogen zu den Themen Demokratie, Nation, Europa, Menschenrechte, Chancengleichheit und Familie auszufüllen, mit dem ermittelt werden soll, welche Kenntnisse und Einstellungen sie zu politischen Themen haben. Weiterhin soll ermittelt werden, wie sie zu diesen Kenntnissen gekommen sind. Daneben werden noch persönliche Daten der Schüler wie z. B. das Geburtsjahr, die Staatsangehörigkeit und das Freizeitverhalten erhoben. Ferner gibt es Fragebögen für die Lehrer und die Schulleitung, mit denen das Umfeld erforscht wird.

Bei dieser Studie gab es vergleichbare datenschutzrechtliche Probleme wie bei der PISA-Studie. Außerdem wurden auch hier die Datenschutzbeauftragten erst sehr spät informiert, so dass eine koordinierte Stellungnahme sehr erschwert wurde. Ich habe auf folgende Punkte hingewiesen:

Erforderlich für die Erhebung personenbezogener Daten im Rahmen der Erhebungsbögen für die Schüler ist die freiwillige und informierte Einwilligung der Eltern, für die die oben bereits darge-

stellten Anforderungen gelten. Die ursprünglichen Mängel in den entsprechenden Informationsschreiben wurden auf Betreiben der Datenschutzbeauftragten weitgehend beseitigt. Insbesondere wird in dem Elternanschreiben nunmehr darauf hingewiesen, dass auch Fragen zur Einschätzung von Erziehungsstilen und Haltungen der Eltern durch die Schüler gestellt werden. Den Eltern wird die Möglichkeit eingeräumt, den Fragebogen in den Schulen einzusehen.

3 Gesundheitswesen

3.1 Allgemeines

3.1.1 Charta der Patientenrechte: Patientenrechte in Deutschland heute

Im Berichtszeitraum wurde auf der Grundlage eines Gutachtens des Instituts für Gesundheits- und Medizinrecht der Universität Bremen und auf Initiative der Gesundheitsminister der Länder in Abstimmung mit den wichtigsten organisierten Beteiligten des Gesundheitswesens ein Entwurf einer „Charta der Patientenrechte“ vorgestellt. Dieses Dokument soll Patienten und Versicherte über ihre wichtigsten Rechte und Pflichten informieren und den Ärzten, Zahnärzten, Pflegekräften und Psychotherapeuten sowie den Mitarbeitern aus Gesundheitsfachberufen in ihrer täglichen Arbeit als Orientierungshilfe dienen. Der Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat an der Überarbeitung dieses Dokuments mitgewirkt; er konnte seine Vorstellungen zumindest teilweise in die Charta einfließen lassen. Auf Betreiben der Bundesärztekammer wurde der Titel der Charta in „Gemeinsamer Standpunkt: Patientenrechte in Deutschland heute“ geändert. Nach dieser Änderung veröffentlichte die Bundesärztekammer dann eine eigene „Patientencharta“.

Der Arbeitskreis Gesundheit und Soziales ist im Rahmen der Diskussionen zum Dokument der Gesundheitsminister - vertreten durch den Hamburger Landesbeauftragten für den Datenschutz - an die federführende Behörde für Arbeit, Gesundheit und Soziales der Freien und Hansestadt Hamburg herangetreten und hat vor allem die Aufnahme dreier aus datenschutzrechtlicher Sicht besonders wichtiger Punkte angeregt:

- Datenschutzrechte des Patienten
- Recht des Patienten auf Nichtwissen
- Beschränkung der Anamneseangaben

Einige Datenschutzrechte der Patienten, wie z. B. das Recht auf Benachrichtigung, auf Auskunft, auf Berichtigung, auf Löschung der Daten und auf technisch-organisatorische Sicherungsmaßnahmen, wurden daraufhin in das Papier aufgenommen. Dagegen fehlen nach wie vor Ausführungen zum Recht auf Nichtwissen, das gerade im Zusammenhang mit genetischen Untersu-

chungen besondere Bedeutung erlangt sowie zur Möglichkeit der Beschränkung von Angaben bei der ärztlichen Anamnese.

Erreicht werden konnte auch, dass die Ausführungen zur Beschränkung des Einsichtsrechts des Patienten bei subjektiven Eindrücken und Wahrnehmungen des Arztes mit dem Zusatz versehen wurden, nach dem Bundesdatenschutzgesetz sei auch dieser Teil der ärztlichen Aufzeichnungen zu offenbaren.

Trotz der oben dargestellten Mängel halte ich das Papier der Gesundheitsminister für einen durchaus gelungenen Ansatz, die Datenschutzrechte der Patienten darzustellen. Wegen des Widerstands der Bundesärztekammer sind die Arbeiten an der Charta bisher nicht zum Abschluss gebracht worden.

Die „Charta der Patientenrechte“ der Bundesärztekammer enthält dagegen einen weit weniger umfassenden Überblick über die Datenschutzrechte der Patienten und deren Beschwerdemöglichkeiten. Z. B. wird zwar das Recht des Patienten auf Einsichtnahme in seine Krankenakte angesprochen, dass dieses Recht jedoch auch durch andere vom Patienten bevollmächtigte Personen ausgeübt werden kann, wird nicht erwähnt. Auch die weitergehende Ansicht der Datenschutzbeauftragten zum Einsichtsrecht des Patienten in subjektive Eindrücke und Wahrnehmungen ist nicht aufgeführt. Die „Patientenrechte auf sorgfältige Information“ sind nur kurz angesprochen und eine umfassende Darstellung der Datenschutzrechte der Patienten fehlt. Das Recht auf Beschränkung der Anmamneseangaben ist ebenfalls nicht enthalten. Lediglich das Recht auf Nichtwissen ist kurz erwähnt.

3.1.2 Gespräch mit Patientenvertretern

Im Rahmen der Diskussion zum Thema „Patientenrechte und Datenschutz“ lud der Arbeitskreis Gesundheit und Soziales, dessen Vorsitz ich innehabe, Vertreter des Gesundheitsladens München e.V. zu einem Gespräch ein. Der Gesundheitsladen ist auch Sitz der Bundesarbeitsgemeinschaft der PatientInnenstellen; er hat einen AK Datenschutz, der sich mit datenschutzrechtlichen Fragen im Gesundheitswesen auseinander setzt. Zur Sprache kamen dabei die verschiedensten

Entwicklungen im medizinischen Bereich, wie z. B. die Vernetzung im Gesundheitswesen und das Gesundheitsreformgesetz 2000 sowie Einzelfragen, wie z. B. das Einsichtsrecht der Patienten in Akten und die häufig wenig datenschutzgerechte Ausgestaltung von Arztpraxen.

Es zeigte sich, dass vielen Patienten die Beschäftigung der Datenschutzbeauftragten mit Gesundheitsfragen nicht bekannt ist. Ich habe gegenüber den Vertretern des Gesundheitsladens meine Aufgaben dargestellt und auf die Bereitschaft der Datenschutzbeauftragten hingewiesen, im Rahmen ihrer Zuständigkeit schwierigen Fällen datenschutzrechtlicher Art nachzugehen.

3.2 Medizinische Forschungsvorhaben

3.2.1 Prospektive Analyse der Drogentoten in Bayern 1999

Ein wissenschaftliches Institut führt ein vom Bayerischen Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit gefördertes Projekt „Analyse der Drogentodesfälle in Bayern“ durch. Ziel dieses Projekts ist es, die Hintergründe zu erhellen, die zum Anstieg der Zahl der Drogentoten in Bayern seit dem Jahr 1997 geführt haben. Das Ministerium trat mit der Bitte an mich heran, die Teilstudie „Prospektive Analyse der Drogentoten in Bayern 1999“ aus datenschutzrechtlicher Sicht zu beurteilen und ggf. Hinweise für eine datenschutzgerechte Ausgestaltung zu geben.

Für diese Studie müssen Informationen über die Lebensumstände der Drogentoten aus verschiedenen Quellen zusammengetragen und verknüpft werden. So werden polizeiliche und staatsanwaltliche Ermittlungsakten gesichtet sowie Institutionen des Drogenhilfesystems, substituierende niedergelassene Ärzte, Angehörige und Personen aus dem sozialen Umfeld des Verstorbenen befragt. Dazu wurden verschiedene Erhebungsbögen entwickelt, die für niedergelassene Ärzte, für Einrichtungen der Drogenhilfe, für die polizeilichen und staatsanwaltlichen Ermittlungsakten und für die Angehörigen des Drogentoten Anwendung finden.

Ich habe in einer Besprechung mit dem Ministerium, dem Forschungsinstitut und weiteren öffentlichen Stellen hervorgehoben, dass zur Übermittlung personenbezogener bzw. personenbeziehbarer Daten der Verstorbenen an das Institut dort eine besondere Offenbarungsbefugnis erforderlich ist, wo die Schweigepflicht der befragten Ärzte, Psychologen, Sozialarbeiter etc. gemäß § 203 Abs. 1 StGB beachtet werden muss. Für die Befragung der Angehörigen und Bekannten des Drogentoten über deren eigene Wahrnehmungen hielt ich grundsätzlich eine Datenerhebung mit deren freiwilliger und informierter Einwilligung für möglich. Wegen der problematischen Frage, ob Angehörige überhaupt in die Verarbeitung medizinischer und sonst besonders geschützter Daten Verstorbener einwilligen können (höchstpersönliches Recht) erzielte ich Einigkeit über die Verwendung eines Pseudonymisierungsverfahrens.

Die Forschenden sind auch hier nicht an personenbezogenen Daten konkreter Personen interessiert, sondern nur an der Möglichkeit, die eine Person betreffenden Daten zusammenzuführen. Letztlich benötigt man hierfür lediglich ein eindeutiges Pseudonym („Codierung"). Sobald die vollständigen Daten je Person vorliegen, kann auf deren Identität gänzlich verzichtet werden.

Vor diesem Hintergrund habe ich daher eine anonymisierte Übermittlung der Daten der Verstorbenen (ohne Name, Adresse und Geburtsdatum) an das Institut angeregt und das Projekt unter Beachtung folgender Maßgaben als datenschutzrechtlich unbedenklich angesehen:

- Zur Zusammenführung der mittels verschiedener Erhebungsbögen erhobenen Daten wird ein 6-stelliger Code verwendet, der sich folgendermaßen zusammensetzt:

  Zweiter Buchstabe des Vornamens, zweiter Buchstabe des Nachnamens, Geschlecht (m/w), letzte Ziffer des Geburtsjahres, letzte Ziffer des Geburtsmonats und letzte Ziffer des Geburtsjahres des Verstorbenen.

- Es dürfen keine personenbezogenen bzw. personenbeziehbaren Daten an das Institut übermittelt werden, um die Schweigepflicht der befragten Ärzte, Psychologen, Sozialarbeiter, etc. nicht in unzulässiger Weise zu durchbrechen.

- In den Erhebungsbögen für die Polizei und die Staatsanwaltschaft, für Einrichtungen der Drogenhilfe, Entgiftungs-Einrichtungen und in dem Interview für Angehörige wird nicht das genaue Geburtsdatum des Verstorbenen sondern nur dessen Geburtsjahr erhoben, um eine ausreichende Anonymisierung im Sinne des Art. 4 Abs. 8 BayDSG zu gewährleisten.

Diesen datenschutzrechtlichen Vorgaben wurde entsprochen.

3.2.2 Forschungs-Studie „Plötzlicher Säuglingstod"

Die vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie geförderte Studie „Plötzlicher Säuglingstod" soll vom November 1998 bis zum Jahr 2002 in zehn deutschen

Ländern bereits bekannte Risikofaktoren für den plötzlichen Säuglingstod näher untersuchen und weitere ermitteln. Der plötzliche Säuglingstod ist mit über 600 verstorbenen Säuglingen pro Jahr die häufigste Todesart im ersten Lebensjahr in Deutschland. Seine Ursachen sind bisher wissenschaftlich weitgehend ungeklärt, der plötzliche Tod kann weder von den Eltern noch von Ärzten vorhergesehen werden.

Die Studie sieht neben einer körperlichen Untersuchung verstorbener Säuglinge (Obduktion) vor, deren Eltern zu den täglichen Gewohnheiten, zur Entwicklung des Kindes, zur Schwangerschaft und zur Geburt, sowie zu weiteren hiermit zusammenhängenden Umständen zu befragen. Diese Befragungen werden von Interviewern durchgeführt, die hierfür eigens geschult wurden. Die Befragung der Eltern erfolgt zuhause und dauert ca. eine Stunde. Daneben werden auch noch „Kontrolleltern“ befragt, um zu erfahren, ob verstorbene und gesunde Säuglinge unter unterschiedlichen Voraussetzungen oder Einflüssen leben. Mit der Auswertung dieser Vergleiche sollen Risikofaktoren aber auch schützende Umstände erkannt werden.

Die Studienzentrale für dieses Projekt befindet sich in der Westfälischen Wilhelms-Universität in Münster. An dem Forschungsvorhaben wirken 14 Universitätsinstitute (Studienzentren) mit. Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen hat gegenüber der Studienzentrale in Münster eine datenschutzgerechte Ausgestaltung der Unterlagen (Aufklärungsschreiben, Einverständniserklärungen, Anschreiben an die Familie mit einem Rückantwortformular und zwei Informationsbroschüren) gefordert. Diese wurden daraufhin so verbessert, dass die Voraussetzungen an eine freiwillige und informierte Einwilligung in die Teilnahme der Erziehungsberechtigten verstorbener Kinder und gesunder Kontrollkinder an der Studie erfüllt waren. Insbesondere wird nunmehr klar gestellt, dass die Teilnahme an der Studie freiwillig ist, die Einwilligung jederzeit ohne Angabe von Gründen widerrufen werden kann und bei einem Widerruf alle gespeicherten Informationen gelöscht werden.

Im Teilprojekt „Totenscheinanalyse“ werden, um auf die Eltern zugehen zu können, Kopien der Todesbescheinigungen aller verstorbenen Kinder im Alter bis zu einem Jahr von den bayerischen Gesundheitsämtern an die Studienzentrale übermittelt. Dies habe ich gem. Art. 3 a Abs. 3 Satz 2 Nr. 2 b des Bayerischen Bestattungsgesetzes (BestG) als zulässig angesehen, da in diesem besonderen Fall das öffentliche Interesse an der Forschung das schutzwürdige Interesse der ver-

storbenen Person erheblich übersteigt, der Zweck der Forschung auf andere Weise nicht erreicht werden kann und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse von Angehörigen der verstorbenen Person an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

3.3 Gesetz über das bevölkerungsbezogene Krebsregister Bayern

Das Gesetz über Krebsregister des Bundes (Krebsregistergesetz - KRG) vom 04. November 1994 (vgl. hierzu im 16. TB, Nr. 2.1.2) trat mit Ablauf des 31. Dezember 1999 außer Kraft. Dasselbe gilt für die hierzu erlassenen bayerischen Ausführungsbestimmungen, das Gesetz zur Ausführung des Krebsregistergesetzes (AGKRG) und die Verordnung zur Durchführung des Krebsregistergesetzes (DVKRG). Zur Weiterführung der Arbeit des bevölkerungsbezogenen (epidemiologischen) Krebsregisters in Bayern war daher eine Nachfolgeregelung notwendig. Das hierfür erlassene Gesetz über das bevölkerungsbezogene Krebsregister Bayern (BayKRG) vom 25. Juli 2000 trat rückwirkend zum 01. Januar 2000 in Kraft. Ich habe im Rahmen des Gesetzgebungsverfahrens zu dem Entwurf Stellung genommen und insbesondere darauf gedrungen, dass das Gesetz nicht hinter den datenschutzrechtlichen Vorgaben des früheren Krebsregistergesetzes zurückbleibt:

- Im Gesetzgebungsverfahren wurde aus finanziellen Erwägungen und aus Gründen der Verwaltungsvereinfachung vorgeschlagen, die bisherige Trennung von Vertrauens- und Registerstelle entfallen zu lassen. Dem habe ich aus datenschutzrechtlicher Sicht mit Erfolg widersprochen:

  Zu einer datenschutzrechtlich vertretbaren Ausgestaltung des Krebsregisters gehört unbedingt die räumliche, organisatorische und personelle Trennung von Vertrauens- und Registerstelle. Dieses System ist wesentlicher Bestandteil der umfassenden Abwägung zweier einander gegenüberstehender Interessen, nämlich der Erforschung von Krebserkrankungen zu deren besseren Bekämpfung einerseits und dem informationellen Selbstbestimmungsrecht der betroffenen Patienten andererseits. Mit dieser Konzeption sowie einem genau geregelten Verfahren der Ver- und Entschlüsselung der Patientendaten, die der Registerstelle nur in nicht personenbezogener Form vorliegen, wird eine Art „informationeller Gewaltenteilung“ als Mittel des Datenschutzes eingesetzt. Der Betroffene hat bei dieser Trennung die Sicherheit, dass seine medizinischen Daten nicht ohne weiteres mit seiner konkreten Person zusammengeführt werden können. Um diesen besonderen Schutz zu gewährleisten, können beide Stellen nicht in einer Dienststelle zusammengefasst werden, da sonst z. B. die Geheim-

haltung der für die Chiffrierung und die Bildung der Kontrollnummern entwickelten und eingesetzten Computerprogramme nicht ausreichend gewährleistet wäre.

Ferner liegt die datenschutzgerechte Ausgestaltung des Krebsregisters nicht nur im Interesse der Patienten, sondern auch im Interesse der Forschung und damit der Allgemeinheit an einer möglichst vollständigen Meldequote. Die Bereitschaft der Patienten, die Tatsache ihrer Erkrankung durch den behandelnden Arzt oder Zahnarzt an ein zentrales Register melden zu lassen, wird durch eine das informationelle Selbstbestimmungsrecht angemessen berücksichtigende Ausgestaltung des Verfahrens sicherlich erleichtert.

- Weiterhin habe ich darauf hingewiesen, dass an dem bisherigen Melderecht der Ärzte und Zahnärzte festgehalten werden sollte. Die Einführung einer Meldepflicht hielte ich aus datenschutzrechtlicher Sicht nur dann für zulässig, wenn Patienten, die in eine solche Meldung nicht einwilligen, nur anonymisiert gemeldet werden. Im BayKRG wurde das Melderecht beibehalten.

- Schließlich begrüße ich es, dass an der grundsätzlichen Informationspflicht des Arztes oder Zahnarztes gegenüber dem Patienten festgehalten wurde. Die einschlägige Bestimmung des BayKRG sieht deren Pflicht vor, den Patienten von einer Meldung zum frühestmöglichen Zeitpunkt - u.a. unter Hinweis auf sein Widerspruchsrecht - zu unterrichten. Nur in begründeten Ausnahmefällen, solange anzunehmen ist, dass dem Patienten gesundheitliche Nachteile entstehen könnten, darf der Arzt oder Zahnarzt von einer Unterrichtung absehen. Die Information des Patienten über sein Widerspruchsrecht dient dazu, ihm eine freie und informierte Entscheidung über die Ausübung dieses Rechts zu ermöglichen. Verschiedentlich wurde von ärztlicher Seite vorgetragen, dass eine allgemeine Information – z. B. über die Medien – genügen müsse. Dieser Auffasssung bin ich unter Hinweis auf die Möglichkeit der Verwendung von Merkblättern entgegen getreten, da sonst von einer informierten Entscheidung bei vielen Patienten nicht mehr die Rede sein kann.

3.4 Datenschutzfragen in Krankenhäusern

3.4.1 Datenschutzgerechte Ausgestaltung eines Krankenhausinformationssystems

Im 18. Tätigkeitsbericht habe ich mich mit der Ausgestaltung der Zugriffsberechtigungen in Krankenhausinformationssystemen (Nr. 3.3.2) und mit dem Krankenhausinformationssystem in den Städtischen Krankenhäusern Münchens (Nr. 3.3.3) beschäftigt. Bei der weiteren Prüfung eines Krankenhauses habe ich mein besonderes Augenmerk auf das dortige Berechtigungskonzept und dessen Umsetzung gerichtet. Die dort bereits über einen längeren Zeitraum erarbeiteten Lösungen sehen derzeit wie folgt aus:

- Ein eigenständiges Berechtigungskonzept gibt es für die Behandlungsdaten im engeren Sinn, das heißt für medizinische Dokumente und Diagnosen. Dieses ist grundsätzlich dahingehend ausgestaltet, dass Ärzte und sonstiges Fachpersonal eine Zugriffsberechtigung auf den Datenbestand lediglich für die Abteilungen erhalten, in denen sie regelmäßig, wenn auch möglicherweise nur „in Vertretung“, tätig sind. Dies sind daher, etwa bei Ärzten, in der Regel mindestens zwei Abteilungen. Die hier vergebenen Berechtigungen sehen in zeitlicher Hinsicht vor, dass das Pflegepersonal noch einen Tag, der Verwaltungsbereich (Schreibkräfte) noch drei Monate und die Ärzte noch sechs Monate nach der Entlassung des Patienten (Sperrfristen) in unterschiedlichem Umfang Zugriff auf den Datenbestand des konkreten Patienten haben; letzteres wird neben der Anfertigung von Arztbriefen insbesondere mit Anfragen von weiterbehandelnden Ärzten und Kostenträgern sowie der Erstellung von Gutachten begründet.

  Darüber hinaus hat das geprüfte Krankenhaus einen behandlungsbezogenen Zugriffsschutz für Dokumente und Diagnosen programmiert. Dies bedeutet, dass die berechtigten Personen außerhalb ihrer oben beschriebenen Berechtigungen unter bestimmten Voraussetzungen (z. B. Notfälle) Zugriff auf Dokumente und Diagnosen anderer Abteilungen und/oder nach dem Beginn der Sperrfrist nehmen können. In beiden Fällen wird der Zugriff aber erst nach Eingabe einer Begründung durch den Zugreifenden freigegeben. Diese Begründung wird protokolliert und das Protokoll wird von der für die Erstellung des Berechtigungskonzepts zuständigen Person auf Plausibilität durchgesehen. Ferner wird die Auswertung an den inter-

nen Datenschutzbeauftragten weitergegeben und bei Bedarf besprochen.

Dieses Konzept halte ich aus datenschutzrechtlicher Sicht für vertretbar und sehr anwenderfreundlich. Die grundsätzliche Beschränkung der Zugriffsberechtigungen der Mitarbeiter eines Krankenhauses auf die jeweilige(n) Abteilung(en) habe ich bereits in meinem 18. Tätigkeitsbericht gefordert. Wünschenswert wäre es, wenn der Programmhersteller diese Erweiterung allgemein anbieten würde.

- Das oben dargestellte Berechtigungskonzept bezieht sich nur auf Diagnosen und Dokumente, jedoch nicht auf den so genannten Stammdatensatz. Dieser orientiert sich am Katalog des § 301 Abs. 1 SGB V. Eine zeitliche Zugriffsbeschränkung auf die Stammdaten im Sinne einer Sperrung ist im Programm nicht vorgesehen. Es können also grundsätzlich alle Personen, die Diagnosen und Dokumente einsehen können, sowie die berechtigten Mitarbeiter der Verwaltung, den Stammdatensatz aller (auch ehemaliger) Patienten des Krankenhauses (ohne zeitliche Einschränkung) einsehen.

  Ich habe hierzu klargestellt, dass aus datenschutzrechtlicher Sicht die Einschränkung des unbegrenzten Zugriffs auf den Stammdatensatz erforderlich ist. Problematisch ist insbesondere, dass die Stammdaten auch längere Zeit nach Verlassen des Krankenhauses abrufbar sind. Zumindest sei die Zugriffsmöglichkeit auf einen stark reduzierten „Kernstammdatensatz“ zu beschränken. Dieser hat sich daran zu orientieren, inwieweit die Daten in Notfällen oder in der Nachtaufnahme erforderlich sind; es muss erkennbar bleiben, dass der Patient bereits im Haus behandelt wurde und welche Abteilung für seine Betreuung zuständig war. Auch diese Zugriffe sollten allerdings protokolliert werden. Das Krankenhaus hat diesen Vorschlag aufgegriffen und einen Antrag auf Entwicklung eines „Kernstammdatensatzes“ an den Entwickler der Software gestellt.

Außerdem habe ich mich im 18. Tätigkeitsbericht zur (teilweisen) Protokollierung der Zugriffe und zur Löschung der im System gespeicherten Daten geäußert (Nr. 3.3.3). Das in dem Krankenhaus eingesetzte KIS bietet nur eine sehr eingeschränkte Möglichkeit der Protokollierung der Zugriffe auf Patientendaten. Nicht protokolliert werden rein lesende Zugriffe auf Stammdaten innerhalb der vergebenen Berechtigung; lediglich im Rahmen des im Krankenhaus selbst pro-

grammierten zusätzlichen behandlungsbezogenen Zugriffsschutzes außerhalb erteilter Berechtigungen bzw. nach Ablauf der Sperrfrist findet eine Protokollierung lesender Zugriffe statt. Stets protokolliert werden dagegen der erste (erstellende) Zugriff und der letzte ändernde Zugriff.

Eine Protokollierung ist zur Feststellung geeignet, ob innerhalb der jeweiligen Berechtigungen missbräuchliche Zugriffe erfolgt sind (Berechtigter greift zu, ohne dass dies erforderlich ist). Besser wäre es aus datenschutzrechtlicher Sicht daher, wenn die lesenden und die ändernden Zugriffe (über die oben geschilderten Fälle hinaus) zumindest stichprobenartig protokolliert werden. Dies wäre auch eine gewisse Hemmschwelle für nicht erforderliche Zugriffe.

Auch zu dieser Frage hat das geprüfte Krankenhaus einen Entwicklungsantrag an den Ersteller der Software gestellt.

Ferner habe ich bei der Prüfung festgestellt, dass eine Löschung der im System gespeicherten Daten nach wie vor nicht vorgesehen ist. Eine solche ist jedoch vor allem im Hinblick auf die Fälle, in denen das Krankenhaus keine Leistung erbracht hat, erforderlich. Solche Fälle liegen z. B. vor, wenn ein Patient vor Erbringung einer Leistung das Krankenhaus wieder verlässt oder in ein anderes Krankenhaus weitergeleitet wird. Auch zur Löschung hat das Krankenhaus einen Entwicklungsantrag gestellt.

3.4.2 Mikroverfilmung von Patientendaten durch einen Privaten

Durch eine Anfrage wurde mir bekannt, dass zwei bayerische Krankenhäuser Mikroverfilmungen von Patientenunterlagen durch eine private Firma durchführen lassen. Verfilmt werden dabei neben den Verwaltungsdaten von Patienten auch deren Behandlungs- bzw. Gesundheitsdaten, medizinische Daten also, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind. Die Verfilmung der Unterlagen erfolgt in einem Raum dieser Firma, der durch eines der Krankenhäuser angemietet wurde. Dieses Krankenhaus hat mit der Firma zudem einen als solchen bezeichneten „Freien-Mitarbeiter“-Vertrag bzw. „Dienstvertrag“ abgeschlossen, durch den der Inhaberin der Firma die Verwahrung sämtlicher Schlüssel zu dem vermieteten Raum übertragen wurde. Zugang zu diesem Raum hat dadurch ausschließlich die Inha-

berin der Firma. Der Raum ist durch entsprechende Schlösser gesichert. Die Krankenhäuser bekommen Zutritt nur über die Inhaberin der Firma. Schließlich wurde der Inhaberin der Firma die Anweisung und Überwachung ihrer Mitarbeiter bei der Vorbereitung und Durchführung der Mikroverfilmung der Patientendaten übertragen.

Ich habe dieses Vorgehen gem. Art. 31 Abs. 1 Satz 1 BayDSG beanstandet, da auch der geltend gemachte Art. 27 Abs. 4 Satz 6 des Bayerischen Krankenhausgesetzes (BayKrG) für diese Vorgehensweise keine Rechtsgrundlage bietet, das Verfahren vielmehr eine Umgehung dieser Vorschrift darstellt.

Patientendaten unterliegen der ärztlichen Schweigepflicht und dürfen ohne Einwilligung des Patienten oder eine sonstige Offenbarungsbefugnis Dritten nicht zur Kenntnis gebracht werden. Nach Art. 27 Abs. 4 Satz 5 BayKrG kann sich ein Krankenhaus zur Mikroverfilmung von Patientendaten anderer Personen oder Stellen bedienen, wenn es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach Art. 27 Abs. 6 BayKrG eingehalten werden und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. Art. 27 Abs. 4 Satz 6 BayKrG bestimmt darüber hinaus, dass zur Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Patienten erforderlich sind (sog. Gesundheitsdaten), sich ein Krankenhaus nur anderer Krankenhäuser bedienen darf. Rechtlicher Hintergrund dieser Bestimmung ist neben der ärztlichen Schweigepflicht insbesondere die Erhaltung des Beschlagnahmeschutzes für diese sensiblen Daten in einem Krankenhaus (§ 97 Abs. 2 Satz 2 StPO).

Art. 27 Abs. 4 Satz 6 BayKrG ist nach der Entscheidung des Bayerischen Verfassungsgerichtshofs vom 6. April 1989 (Az.: Vf. 2-VII-87; BayVBl 1989, 397) verfassungsgemäß. Das Gericht hat unter anderem ausgeführt, dass diese Bestimmung es den Krankenhäusern nicht verwehre, medizinische Daten in einer dem Art. 26 Abs. 4 Satz 5 BayKrG a.F. (jetzt: Art. 27 Abs. 4 Satz 6 BayKrG) entsprechenden Ausgestaltung innerhalb des Krankenhauses durch Dritte mikroverfilmen zu lassen. Die gegen diese Entscheidung gerichtete Verfassungsbeschwerde wurde vom Bundesverfassungsgericht im Beschluß vom 25. September 1990 nicht zur Entscheidung angenommen (NJW 1991, 2952).

Nach dem Wortlaut und Sinn und Zweck des Art. 27 Abs. 4 Satz 6 BayKrG ist die Mikroverfilmung medizinischer Behandlungsdaten nur in einem Krankenhaus zulässig. Deren Mikroverfilmung durch Private außerhalb eines Krankenhauses scheidet daher aus. Datenschutzrechtlich hinnehmbar wäre es allenfalls, wenn der angemietete Raum zweifelsfrei einem der Krankenhäuser (oder beiden) zugeordnet werden könnte. Hierfür müsste dieses die „Schlüsselgewalt“ über den Raum auch tatsächlich inne haben. Die Schlüssel für den angemieteten Raum müssten im „alleinigen“ Gewahrsam des Krankenhauses bleiben. Die Mitarbeiter der Firma einschließlich der Inhaberin selbst dürften keinen Schlüssel für diesen Raum besitzen. Ausschließlich die Krankenhäuser bzw. deren befugte Mitarbeiter müssten den Zugang zu diesem Raum gewähren. Öffnen dürften ihn nur befugte Mitarbeiter der Krankenhäuser zur Durchführung der Mikroverfilmung. Bei dieser Mikroverfilmung müssten die Beschäftigten der Firma unter Aufsicht und nach den Anweisungen eines Mitarbeiters des jeweiligen Krankenhauses arbeiten, der darauf zu achten hat, dass den Mitarbeitern der Firma möglichst keine Gesundheitsdaten zur Kenntnis gelangen. Nach Durchführung der Mikroverfilmung wäre der Raum wieder sorgfältig zu verschließen. Diese Anforderungen wären vertraglich festzulegen.

Die in dem geschilderten Fall gewählte „Anmietungslösung“ kann nicht bewirken, dass der vermietete Raum als Raum im Krankenhaus anzusehen ist, da die Inhaberin der Firma uneingeschränkt Zugang zu diesem Raum hat. Ferner bleiben auch die Schlüssel in ihrem Gewahrsam. Es wird nur gewährleistet, dass das Krankenhaus Zutritt erhält, wenn es ihn für erforderlich hält. Der angemietete Raum kann daher von der Ausgestaltung der Abläufe nicht einem der Krankenhäuser zugeordnet werden. Diese können auch nicht jederzeit darüber entscheiden, wer den Raum wann betreten kann, da die Inhaberin der Firma – nicht die Krankenhäuser – die „Schlüsselgewalt“ inne hat.

Es ist also keine der geschilderten Voraussetzungen, unter denen eine Mikroverfilmung medizinischer Behandlungsdaten durch einen Privaten ausnahmsweise hinnehmbar ist, erfüllt. Mit dem Abschluss des „Freien-Mitarbeiter“-Vertrags wird ein Gewahrsam des Krankenhauses nicht erreicht. Die Regelungen des Vertrags enthalten nichts anderes als das, was auch für eine Auftragsdatenverarbeitung nach Art. 6 BayDSG zu regeln wäre. Die Inhaberin der Mikroverfilmungsfirma selbst zu einer Mitarbeiterin der Krankenhäuser machen zu wollen, bezweckt lediglich Art. 27 Abs. 4 Satz 6 BayKrG zu umgehen. Sinn und Zweck der Mikroverfilmung durch

einen Dritten unter Aufsicht und nach den Anweisungen eines (originären) Mitarbeiters des Krankenhauses ist es nämlich, soweit wie möglich zu verhindern, dass unbefugte Dritte der ärztlichen Schweigepflicht unterliegende Gesundheitsdaten zur Kenntnis nehmen können. Diese Kontrollfunktion ist jedoch dann nicht gewährleistet, wenn der die Mikroverfilmung Durchführende sich selbst kontrolliert.

3.4.3 Weitergabe der Namen von Patienten der Herzchirurgie einer Klinik an eine Stiftung

Wie mir durch Presseartikel bekannt wurde, übermittelte der Chefarzt der Abteilung für Herzchirurgie eines Klinikums eine Diskette mit den Namen und Adressen von über 2500 ehemaligen Patienten an eine private Stiftung. Zweck dieser Weitergabe personenbezogener Daten war die Versendung von Bittbriefen zugunsten der Stiftung, unter Verwendung des Briefkopfs des Klinikums, um ein Ultraschallgerät für die Nutzung im Klinikum beschaffen zu können.

Ich habe diese Übermittlung der Namen und Adressen ehemaliger Patienten als unbefugte Übermittlung von Patientendaten bewertet und gemäß Art. 31 Abs. 1 Satz 1 BayDSG beanstandet.

Die Namen und Adressen ehemaliger Patienten sind Geheimnisse, die der ärztlichen Schweigepflicht unterliegen, da sich hieraus auf die Tatsache eines Aufenthalts oder einer Behandlung der Personen in der Herzchirurgie des Klinikums schließen lässt. Diese Offenbarungen geschahen auch unbefugt. Eine befugte Übermittlung von Patientendaten erfordert das Vorliegen einer Offenbarungspflicht oder einer Offenbarungsbefugnis. Offenbarungspflichten kamen nicht in Betracht.

Die Voraussetzungen des Art. 27 Abs. 5 Satz 1 des Bayerischen Krankenhausgesetzes (BayKrG) lagen ebenfalls nicht vor. Nach dieser Vorschrift, der wichtigsten Offenbarungsbefugnis für bayerische Krankenhäuser, ist die Übermittlung von Patientendaten an Dritte insbesondere zulässig im Rahmen des Behandlungsverhältnisses oder dessen verwaltungsmäßiger Abwicklung oder wenn eine Rechtsvorschrift die Übermittlung erlaubt oder wenn die betroffenen Personen einge-

willigt haben. Diese Voraussetzungen lagen nicht vor. Zwar könnte grundsätzlich auch eine mutmaßliche Einwilligung eines Patienten in Frage kommen. Das konnte man hier jedoch bei der Fülle der Betroffenen nicht für jeden einzelnen Fall annehmen. Eine mutmaßliche Einwilligung kommt nur dann in Betracht, wenn im vermeintlichen Interesse und Einverständnis des geheimnisgeschützten Patienten gehandelt worden wäre. Das kann hier jedoch nicht für sämtliche Patienten unterstellt werden, zumal die beabsichtige Anschaffung des Ultraschallgerätes vornehmlich im Interesse künftiger Patienten liegen dürfte.

3.5 Telemedizin

Wie ich bereits für den letzten Berichtszeitraum (vgl. Nr. 3.4 des 18. TB) feststellen konnte, schreitet die Entwicklung und Ausbreitung der Telemedizin weiter voran. Ich habe mich erneut an zahlreichen Diskussionen in maßgeblichen Gremien beteiligt und verschiedene Projektträger bei der datenschutzgerechten Ausgestaltung telemedizinischer Anwendungen beraten.

Mehrere Einrichtungen der Selbstverwaltung des Gesundheitswesens gründeten im August 1999 unter dem Dach der Gesellschaft für Versicherungswissenschaft und -gestaltung e.V. (GVG) in Zusammenarbeit mit den Bundesministerien für Gesundheit (BMG) und für Bildung und Forschung (BMBF) das „Aktionsforum Telematik im Gesundheitswesen“ (ATG) als Konsensplattform für die Weiterentwicklung der Telematik im Gesundheitswesen. Das ATG will die Systembeteiligten zusammenführen, Konsensmöglichkeiten aufzeigen und Empfehlungen erarbeiten, die den Partnern und den zuständigen Ministerien als Orientierung dienen sollen. Es will Vorschläge und Empfehlungen zur organisatorisch-technischen Infrastruktur sowie zu den Standards dieser Infrastruktur ausarbeiten.

Zu diesem Zweck hat das ATG im Februar 2000 vier Teams zu den Themenbereichen „Elektronisches Rezept“, „Elektronischer Arztbrief“, „Sicherheitsinfrastruktur“ und „Europäische und internationale Dimension von Telematik im Gesundheitswesen“ eingesetzt. Mit Hilfe dieser Teams will es Handlungsempfehlungen für die Selbstverwaltung und ggf. für die Gesetzgebung im Form von „Managementpapieren“ erstellen. Die Papiere sind im Internet (http://atg.gvg-koeln.de) abrufbar und können dort auch öffentlich kommentiert werden.
Ich habe sowohl aus technischer als auch aus rechtlicher Sicht zu diesen Papieren Stellung genommen. Aus datenschutzrechtlicher Sicht habe ich nochmals hervorgehoben, dass die Möglichkeit und der Wunsch Telemedizin zu betreiben, nichts an den rechtlichen Grundlagen der Datenverarbeitung in der Medizin ändern. Alleine der Wunsch nach Umsetzung telemedizinischer Anwendungen kann die hiermit verbundenen Datenverarbeitungen nicht rechtfertigen. Auch in der Telemedizin gelten die selben rechtlichen Regelungen wie in der traditionellen – nicht vernetzten – Medizin. Zu beachten ist daher die in den Berufsordnungen für die Ärztinnen und Ärzte geregelte ärztliche Schweigepflicht, die in § 203 Abs. 1 Nr. 1 StGB strafbewehrt ist.

Grundlage ist ferner der Grundsatz der Erforderlichkeit, der stets verlangt, danach zu fragen, ob überhaupt personenbezogene Daten verwendet werden müssen oder nicht etwa anonymisierte oder pseudonymisierte Daten (z.B. für Qualitätssicherungsverfahren) ausreichen. Sollte dennoch die Übermittlung personenbezogener Daten erforderlich sein, stellt sich die Frage, in welchem Umfang ärztliche Informationen übermittelt werden müssen. Für personenbezogene oder personenbeziehbare Datenverarbeitungen sind der Behandlungsvertrag, die (freiwillige, informierte und in der Regel schriftliche) Einwilligung des Patienten, sowie die bereichsspezifischen (z. B. Krankenhausgesetze) und die allgemeinen Datenschutzgesetze zu beachten. Je nach Anwendungsbereich ist die ärztliche Kommunikation ggf. auch in den einzelnen Büchern des Sozialgesetzbuches (SGB) geregelt, vgl. etwa § 73 Abs. 1b SGB V (Hausarztmodell) und § 140a Abs. 2 SGB V (Integrierte Versorgung).

Bezüglich der Einwilligung des Patienten ist durch die technische Ausgestaltung der Verfahren sicher zu stellen, dass keine Übermittlung von personenbezogenen Patientendaten ohne Einwilligung erfolgt und sich die Kommunikation zwischen den Leistungserbringern am konkreten Behandlungsbezug orientiert. Es ist zu verhindern, dass ein Patient, der sich einer telemedizinischen Behandlung unterzieht, seine medizinischen Daten pauschal gegenüber allen beteiligten Leistungserbringern offenbaren muss. Eine generelle und vorab für alle Behandlungen erklärte Einwilligung des Patienten in die künftige Verarbeitung seiner medizinischen Daten, deren Umfang und Tragweite er zum Zeitpunkt der Erklärung nicht übersehen kann, ist nicht zulässig. Darüber hinaus müssen die allgemeinen rechtlichen Anforderungen an Einwilligungserklärungen beachtet werden. Insbesondere müssen die Betroffenen über Umfang und Zweck der vorgesehenen Verarbeitung ihrer Daten konkret informiert werden. Die Einwilligung muss in der Regel schriftlich erteilt werden. Ferner ist ein vorausgehender Hinweis durch den behandelnden Arzt bzw. andere Leistungserbringer erforderlich, dass die Einwilligung freiwillig und ein Widerruf möglich ist.

Das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit hat im Berichtszeitraum beschlossen, ein ständiges Forum von Experten einzuberufen, das der Entwicklung der Telemedizin in Bayern eine Plattform bietet. In dieser „Plattform Telemedizin in Bayern“ sollen Fachleute bayernweit sämtliche telemedizinischen Aktivitäten bündeln und bewerten. Die Plattform soll im Unterschied zu einem bereits bestehenden Themenarbeitskreis Telemedizin unabhängig von der Laufzeit einzelner Projekte und auch unabhängig von der „Offen-

sive Zukunft Bayern“ fortbestehen. In den Treffen der Plattform wird über laufende Projekte, unter anderem aus dem Programm Bayern Online II, berichtet; es werden weitere Projekte vorgestellt und bewertet. Ich habe an diesen Treffen teilgenommen und auf die datenschutzrechtlichen Anforderungen der Telemedizin hingewiesen.

Aber auch die praktische Umsetzung der Telemedizin hat Fortschritte gemacht. Im Rahmen der Initiative Bayern Online II hat das Kabinett die weitere Förderung telemedizinischer Projekte bewilligt. Z.B. werden in Nürnberg vier Projekte zur Betreuung von Diabetespatienten, zur flächendeckenden Schlaganfallversorgung, zur Telepathologie und zur Vernetzung Praxis/Klinik gefördert. Insgesamt befassen sich nach einer Auskunft des Staatsministeriums für Wissenschaft, Forschung und Kunst alleine die fünf bayerischen Universitätskliniken mit über 100 Projekten zur Telemedizin.

Von den von mir datenschutzrechtlich beratenen Projektträgern möchte ich exemplarisch nur folgende Projekte nennen:

- Das Projekt „Bayerische Gesundheitschipkarte und Kommunikation“ (BGK) will einen Einstieg in die Nutzung von Patientenkarten schaffen. In einer ersten Anwendungsebene sollen verschiedene Routineanwendungen, wie z. B. die Überweisung, die Einweisung, die Entlassung, der Arztbrief und das Rezept in die Chipkartentechnologie umgesetzt werden. In einer späteren zweiten Anwendungsebene sollen dann komplexere Kommunikationsansprüche bewältigt werden. In einer Besprechung mit den Betreibern dieses Verfahrens habe ich u.a. auf die datenschutzrechtlichen Anforderungen der Nutzung von Chipkarten im Gesundheitswesen (vgl. auch den 17. TB, Nr. 3.1.1) hingewiesen.

- Im Rahmen des Projekts „Telemedizin in Ostbayern“ finden u.a. so genannte „Telekonsile“ statt. Dabei wendet sich der anfragende Arzt direkt an einen ihm bekannten Spezialisten der Uniklinik Regensburg. Die Konsile laufen unter Wahrung der Anonymität des Patienten, dennoch wird vorher seine Einwilligung eingeholt. Bei der Beratung des Projekts habe ich klar gestellt, dass einem Konsiliarius in der Regel keine patientenbezogenen Geheimnisse offenbart werden müssen. Sollte dies im Einzelfall doch erforderlich sein, müsste eine Offenbarungsbefugnis vorliegen. Da ein Konsiliarius nicht vor-, mit- oder nachbehandelnder Arzt

ist, liegen bei Krankenhausärzten die Voraussetzungen der Art. 27 Abs. 5 Satz 2 BayKrG in der Regel nicht vor. Deshalb empfiehlt sich das Einholen der (ausdrücklichen) Einwilligung des Patienten. In Einzelfällen (Notfälle, Bewusstlosigkeit etc.) halte ich es aus datenschutzrechtlicher Sicht für zulässig, eine mutmaßliche Einwilligung des Patienten anzunehmen, wenn der Arzt im Interesse und mit dem mutmaßlichen Einverständnis des Betroffenen handelt und kein entgegenstehender Wille des Patienten erkennbar ist.

In dem Projekt „Neue Kommunikationstechnologien in der Notfallmedizin“ (NOAH II) will das Universitätsklinikum Regensburg in Zusammenarbeit mit dem Landkreis Cham und dem Telezentrum in Stamsried ein flächendeckendes multimediales Kommunikationsnetz in der Region Ostbayern mit Einbindung zahlreicher Krankenhäuser sowie Praxen aufbauen.

- Das Projekt „ENDOTEL“ der TU München bietet die Telekonsulation, die Telediagnostik und die Teleausbildung im Bereich der Endoskopie an.

3.6 Patienten-Verlaufsinformation vom aufnehmenden Krankenhausarzt an den Patienten überbringenden Notarzt

Die Bayerische Landesärztekammer ist mit der Frage an mich herangetreten, ob eine sog. „Rückwärtsinformation“ vom aufnehmenden Krankenhausarzt an den Patienten überbringenden Notarzt datenschutzrechtlich zulässig sei. Inhaltlich ging es dabei im Wesentlichen um folgende Fragestellung: Ein Notarzt behandelt einen Patienten im Rahmen der Erstversorgung. Nach der Einlieferung dieses Patienten in ein Krankenhaus bricht im Regelfall der Kontakt zwischen beiden ab, sodass der Notarzt die Qualität seiner ärztlichen Hilfsmaßnahmen nicht beurteilen kann. Die Bayerische Landesärztekammer wollte wissen, ob es aus datenschutzrechtlicher Sicht möglich wäre, dem Notarzt diesbezügliche Informationen (weiterer Krankheitsverlauf etc.) für seine (individuelle) Qualitätssicherung zu übermitteln.

Die damit verbundenen Fragen wurden im Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder diskutiert, wobei sich herausstellte, dass eine bundeseinheitliche Lösung wegen der unterschiedlichen landesgesetzlichen Regelungen ausscheidet. Weiterhin fand unter meiner Beteiligung eine Besprechung mit Vertretern der Bayerischen Staatsministerien des Innern und für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit bei der Bayerischen Landesärztekammer statt. Das wesentliche Ergebnis dieser Unterredung erschien bereits im Oktoberheft 1999 des Bayerischen Ärzteblatts. Folgende Stichpunkte der datenschutzrechtlichen Bewertung betrachte ich als wesentlich:

– Weder das Bayerische Krankenhausgesetz (BayKrG) noch das Bayerische Rettungsdienstgesetz (BayRDG) enthält eine spezielle Rechtsgrundlage für die „Rückwärts-Information“, die es einem Notarzt ermöglicht, die erforderlichen Patientendaten von einem Krankenhaus ohne (ausdrückliche) Einwilligung des Patienten zu erhalten.

– Art. 27 Abs. 5 Satz 2 BayKrG bestimmt allerdings u.a., dass eine Offenbarung von Patientendaten an Vorbehandelnde zulässig ist, soweit das Einverständnis der Patienten anzunehmen ist. Aus datenschutzrechtlicher Sicht halte ich es für einen gewissen Übergangszeitraum bis zur Schaffung einer klaren Rechtsgrundlage für vertretbar, aufgrund dieser Regelung be-

stimmte Patientendaten innerhalb eines eng begrenzten Zeitraums nach dem Notfall (bis max. 48 Stunden) durch das Krankenhaus an den Notarzt zu übermitteln, soweit diese Daten für dessen individuelle „Qualitätssicherung“ erforderlich sind. Die Übermittlung muss sich auf aus medizinischen Gründen erforderliche Patientendaten beschränken. Die Erforderlichkeit ist aus medizinischer Sicht zu beurteilen. Solange es sich lediglich um die Aktualisierung bereits vom Notarzt erhobener Daten (Verlaufswerte) handelt, spricht vieles dafür, dass diese Befunde abgefragt werden können, da insoweit die Annahme des mutmaßlichen Patienteneinverständnisses vertretbar erscheint, es sei denn, es liegen gegenteilige Hinweise vor.

– Sollte allerdings die Einwilligung eines Patienten eingeholt werden können, geht diese Möglichkeit vor. Der Patient sollte – soweit möglich – über dieses Vorhaben informiert werden. Ein Widerspruch des Patienten wäre zu beachten. Schließlich dürfen die übermittelten Daten grundsätzlich auch nicht gespeichert werden, da sie nur der persönlichen Qualitätskontrolle des Notarztes dienen.

– Auf Dauer halte ich allerdings nach wie vor die Schaffung einer normenklaren gesetzlichen Grundlage für dieses Verfahren für notwendig.

3.7 Qualitätssicherungsprojekte

3.7.1 Qualitätssicherung im medizinischen Bereich

Auch im medizinischen Bereich werden immer häufiger Qualitätssicherungsprojekte durchgeführt. Sie nehmen dort datenschutzrechtlich insofern keine Sonderstellung ein, als eine personenbezogene oder personenbeziehbare Offenbarung von Patientendaten auch hier nur bei Vorliegen einer Offenbarungsbefugnis zulässig ist, da auch die hier verarbeiteten Daten i.d.R. der ärztlichen Schweigepflicht unterfallen. Da es - zumindest in Bayern – keine (besondere) gesetzliche Offenbarungsbefugnis gibt (z.B. im BayKrG) und die Einwilligungen aller betroffenen Patienten meist nicht eingeholt werden können, habe ich grundsätzlich darauf gedrungen, dass die auszuwertenden Daten i.S. des Art. 4 Abs. 8 BayDSG ausreichend anonymisiert werden.

- Die Bayerische Arbeitsgemeinschaft für Qualitätssicherung in der stationären Versorgung (BAQ) führt u.a. ein Qualitätssicherungsprojekt im Bereich der Peri- und Neonatologie durch. Ziel dieses Vorhabens ist die kontinuierliche Verbesserung der Behandlungsqualität. Hierzu werden Daten von Müttern und Neugeborenen an die BAQ übermittelt, zum Teil mit Erhebungsbögen, die von den mitwirkenden Krankenhäusern ausgefüllt werden, zum Teil mit EDV-Unterstützung. Bei der Datenübermittlung mit Erhebungsbögen erfolgt die zur Datenverarbeitung erforderliche Datenerfassung durch die BAQ, die die Daten auch auf ihre Plausibilität überprüft; anschließend werden die Erhebungsbögen vernichtet.

  Die Datenübermittlung in Papierform ist aus datenschutzrechtlicher Sicht problematisch. Vom Personal der Krankenhäuser werden in den Bögen zwar weder die Namen oder die Adresse von Mutter und Kind noch das Geburtsdatum der Mutter, wohl aber weitere genaue Zeitpunkte (z.B. der Geburt des Kindes, der Entlassung bzw. Wiederaufnahme von Mutter und Kind etc.) erfasst, obwohl für die Qualitätssicherung an sich die Ermittlung bestimmter Zeiträume ausreichen würde. Durch das genaue Erfassen dieser Zeitpunkte wird jedoch das Risiko einer Deanonymisierung von Mutter und Kind erheblich vergrößert. Durch die EDV-gestützte Lösung können diese Probleme weitgehend vermieden werden, da bereits bei der Eingabe Zeiträume errechnet und nur diese an die BAQ weitergegeben werden. Die papiergestützte Übermittlung ist daher nur als Übergangslösung anzusehen,

die zunehmend - soweit die mitwirkenden Krankenhäuser hierzu in der Lage sind - abgelöst werden muss. Die BAQ hat mir versichert, dass eine solche EDV-gestützte Übermittlung auch in ihrem Interesse ist, da sie den eigenen Arbeitsaufwand deutlich reduziere.

In den von der BAQ verwendeten Erhebungsbögen ist zur Erlangung gebietsbezogener Auswertungsergebnisse die Übermittlung der um die letzte Stelle gekürzten Postleitzahl des Wohnorts von Mutter und Kind vorgesehen. Aus datenschutzrechtlicher Sicht ist die Übermittlung eines Erhebungsbogens mit der vollen Postleitzahl nicht zulässig, da es keine gesetzliche Grundlage für eine Übermittlung dann häufig personenbeziehbarer Daten an die BAQ gibt. Eine Übermittlung genauer Postleitzahlen würde nämlich - vor allem im ländlichen Bereich - den Kreis der Betroffenen häufig so stark einengen, dass eine Deanonymisierung nicht mehr auszuschließen wäre.

- Ferner wurde ich zur datenschutzrechtlichen Beratung für das Projekt „Freiwillige Krankenhausvergleiche zur externen Qualitätssicherung in der Psychiatrie“ herangezogen. Es handelt sich hierbei um ein Modellprojekt zur externen, freiwilligen Qualitätssicherung für Einrichtungen, die in der stationären Psychiatrie tätig sind. Hierzu werden die sog. BADO-Daten, die der internen medizinischen Basisdokumentation dienen, zumindest teilweise an die auswertende Stelle im Bezirksklinikum Regensburg übermittelt.

  Von dem BADO-Datensatz werden z.B. der Name, der Vorname und der Geburtsname gestrichen. Das Geburtsdatum wird durch eine Patientenidentifikationsnummer (PIN) ersetzt. Ferner werden die Daten Geburtsort, Beruf, Straße, Hausnummer, Postleitzahl, Wohnort, Telefonnummer, Staat, Familienstand und Religion nicht übermittelt. Übermittelt wird dagegen die sog. Gemeindekennzahl, so dass in der Regel der Name des Landkreises aus dem der psychiatrische Patient stammt, weitergegeben wird. Ich habe hierzu ausgeführt, dass das Vorhaben den Anforderungen an eine ausreichende (faktische) Anonymisierung genügt, wenn folgende Voraussetzungen erfüllt sind:

  - Die oben angesprochene PIN wird generiert, um Datensätze aus verschiedenen Quellen zu einer Person (möglichst) eindeutig zusammenführen zu können. Interessant für die auswertende Stelle ist nicht der Patient an sich, sondern nur der Fall. Mit

der PIN werden der Vorname, der Familienname, das Geschlecht und das Geburtsdatum codiert und durch zwei Ziffern ergänzt, um unterschiedliche Personen zu bezeichnen, so dass es nicht mehr möglich ist, hieraus auf diese Daten zu schließen. Ich habe darauf hingewiesen, dass sich aus der PIN keine weiteren personenbezogenen Daten, insbesondere nicht das Geburtsdatum des Patienten, ergeben dürfen. Die Codierung des Geburtsdatums erfolgt so, dass die Anzahl der Tage zwischen einem Referenzdatum und dem Geburtsdatum der Person zugrunde gelegt wird. Da es genügt, ein beliebiges Datum als Geburtsdatum durch das Programm umwandeln zu lassen und den dafür erzeugten Code (Zahlenwert) zurückzurechnen, wäre es möglich, jeweils das genaue Geburtsdatum zu berechnen. Ich habe daher vorgeschlagen, die Rechenvorschrift um wenigstens eine, nur dem Programmierer bekannte komplexere mathematische Operation zu erweitern, damit das Geburtsdatum nicht mehr so trivial zu berechnen wäre. Dies wurde mir bestätigt.

- Hinsichtlich der Übermittlung der Gemeindekennzahl habe ich keine datenschutzrechtlichen Bedenken, falls diese grundsätzlich um drei Stellen gekürzt wird, so dass als kleinste Einheit der Landkreis erscheint.

- Hinsichtlich einer verschlüsselten Übertragung der Daten per e-mail hat das Bezirksklinikum Regensburg vorgeschlagen, dass die Identifikations- und Behandlungsdaten getrennt und jeweils verschlüsselt an das Klinikum geschickt werden sollten. Bei Verwendung eines sicheren Verschlüsselungsprodukts habe ich gegen dieses Vorgehen keine Bedenken. Um auch die Authentizität und die Integrität der übermittelten Daten sicherzustellen, sollten diese digital signiert werden.

3.7.2 Gutachterliche Struktur- und Trendanalyse des Rettungsdienstes in Bayern

Einige Sozialverbände sind mit dem Wunsch an mich herangetreten zu prüfen, ob die vom Bayerischen Staatsministerium des Innern bei dem Klinikum Innenstadt der Ludwig-Maximilians-Universität München in Auftrag gegebene „Gutachterliche Struktur- und Trendanalyse des Rettungsdienstes in Bayern“ den datenschutzrechtlichen Bestimmungen entspricht. Mit dieser Analyse des Rettungsdienstes sollen Vorschläge für die Optimierung der rettungsdienstlichen Vorhaltung unter Vermeidung eines weiteren erheblichen Kostenanstiegs erarbeitet werden. Hierzu soll eine Bestandsaufnahme sowie eine exakte Erfassung des Einsatzgeschehens erfolgen. Dafür werden sowohl Daten von Patienten als auch vom Personal der Rettungsdienste an die Gutachter übermittelt. Aus datenschutzrechtlicher Sicht war insbesondere auf eine hinreichende Anonymisierung dieser Daten hinzuwirken.

Ich habe in einer Besprechung mit Vertretern des Ministeriums, des Klinikums und anderer Stellen zunächst zum Ausdruck gebracht, dass eine Rechtsgrundlage für die Übermittlung personenbezogener Daten an das Klinikum nicht ersichtlich und eine Einwilligungslösung i.d.R. nicht realisierbar sei. Um die daher für die Datenübermittlung notwendige faktische Anonymisierung der namentlich nicht bekannten Betroffenen zu erreichen, bestand Einigkeit über folgendes Vorgehen:

- Auf die Übermittlung des Geschlechts der transportierten Personen wird verzichtet.

- Auch auf die Übermittlung des Geburtsdatums der transportierten Personen wird verzichtet. Datenschutzrechtlich zulässig ist die Übermittlung des Geburtsjahrs oder Lebensalters (in Jahren) der Patienten.

- Bezüglich der Daten zum Ausgangs- und Endpunkt der Transporte entfällt die Übermittlung der Hausnummern. Unbedenklich ist dagegen die Übermittlung der jeweiligen Straßennamen und einer noch zu erarbeitetenden Bezeichnung für Wachbereiche. Dies sind die bestehenden Zuständigkeitsbereiche von Rettungswachen.

- Im Hinblick auf die Befürchtung, dass aufgrund der zu übermittelnden Daten auch eingesetztes Personal der Rettungsdienste identifiziert werden könne, war ich angesichts der Tatsache, dass dem Gutachter keine Dienstpläne der Rettungsdienste übermittelt werden, der Auffassung, dass eine Identifizierung des eingesetzten Personals nicht möglich sei.

Unter Beachtung dieser Maßgaben hatte ich gegen eine Übermittlung der Daten anhand der überarbeiteten Datenlisten keine datenschutzrechtlichen Bedenken, weil die insoweit reduzierten Übermittlungen keine personenbezogenen Daten im Sinne des Art. 2 Abs. 1 BayDSG umfassen, da sie keine Angaben über Verhältnisse bestimmter oder bestimmbarer Personen enthalten.

3.8 Datenschutz in den Gesundheitsabteilungen der Landratsämter

Ich habe mich bereits in früheren Tätigkeitsberichten (vgl. 10. TB, Nr. 2.3; 11. TB, Nr. 2.2; 13. TB, Nr. 2.2, 14. TB, Nr. 2.1; 15. TB, Nr. 2.4; 16. TB, Nr. 2.4 und 17. TB, Nr. 3.5) mit in Gesundheitsämtern auftretenden datenschutzrechtlichen Fragen beschäftigt. Insbesondere die Eingliederung der staatlichen Gesundheits- und Veterinärämter in die Landratsämter wirft datenschutzrechtliche Fragen auf. Ich weise hierzu auf die genannten Ausführungen im 17. TB hin. Datenschutzrechtliche Leitlinie dieser Eingliederung muss sein, dass sie für die Betroffenen nicht zu einer Verschlechterung ihrer datenschutzrechtlichen Position gegenüber dem früheren Zustand führen darf.

Im Einzelnen ist mir bei der Prüfung der Gesundheitsabteilung eines Landratsamts Folgendes aufgefallen:

- Für die interne Organisation der Gesundheitsabteilung eines Landratsamtes gibt es Mustergeschäftsverteilungspläne für die Landratsämter in der Bekanntmachung des Bayerischen Staatsministeriums des Innern vom 04. Januar 1996 (IZ7-0211.4). Die dort vorgeschlagene Aufteilung der Gesundheitsabteilung in drei Sachgebiete entspricht den datenschutzrechtlichen Anforderungen des Art. 6 Abs. 1 Satz 5 Gesundheitsdienstegesetz (GDG), wonach die Wahrung der Geheimhaltungspflichten und Verwertungsverbote durch angemessene Maßnahmen auch organisatorisch sicher zu stellen ist. Die organisatorische Absicherung des Verwertungsverbots des Art. 6 Abs. 1 Satz 1 GDG erfolgt dadurch, dass einem Sachgebiet der Bereich der freiwilligen gesundheitlichen Aufklärung und Beratung, der einem besonderen Schutz unterliegt, übertragen ist. Dagegen obliegen die hoheitlichen Aufgaben weitgehend den beiden anderen Sachgebieten.

- Hinsichtlich der datenschutzgerechten Ausgestaltung der Schwangeren(-konflikt)beratung weise ich zunächst auf den 16. TB (Nr. 2.4.2) und den 17. TB (Nr. 3.5.1, Ziffer 4) hin. Im Rahmen der Prüfung hat sich gezeigt, dass nicht alle datenschutzrechtlichen Anforderungen erfüllt waren:

- Nach dem Bayerischen Schwangerenberatungsgesetz (BaySchwBerG) soll möglichst frühzeitig, jedenfalls vor Beginn des Beratungsgesprächs, in geeigneter Weise über die umfassende Schweige- und Geheimhaltungspflicht aller in der Beratungsstelle tätigen Personen und die Möglichkeit der anonymen Beratung informiert werden. Dafür bietet sich bereits in der Regel die telefonische Vereinbarung eines Gesprächstermins an. Ferner sollten ein oder mehrere deutlich sichtbare Schilder im Eingangsbereich der Beratungsstelle angebracht werden, die die Frauen auf die Schweigepflicht und auf die Möglichkeit der anonymen Beratung aufmerksam machen. Ferner darf im Terminkalender der Berater kein Name, sondern nur ein Sachvermerk (z. B. § 218) angebracht werden.

- Wichtig für die Anonymität der Beratung ist auch die räumliche Unterbringung der Beratungsstelle. In der geprüften Gesundheitsabteilung befinden sich die Zimmer der Berater im Erdgeschoss im Eingangs- und Wartebereich der Gesundheitsabteilung. Für dort Wartende ist es ohne weiteres erkennbar, dass und welche Frauen zur Schwangerenberatung kommen. Dies wird allenfalls dadurch abgemildert, dass die Frauen bei der Terminabsprache am Telefon auf den genauen Weg zu den Beratungszimmern hingewiesen werden. Die Anonymität der Schwangerenberatung könnte besser gewährleistet werden, z. B. durch ein Verlegen der Beratungszimmer in ein oberes Stockwerk, durch das Verlegen des allgemeinen Wartebereichs oder durch das Schaffen eines eigenen – abgetrennten – Wartebereichs.

  Außerdem habe ich bei meiner Kontrolle festgestellt, dass - zumindest einige - Zimmer der Berater von Passanten der vorbeiführenden Fußgängerzone aus eingesehen werden können und die Lamellenrollos wegen des dann fehlenden Tageslichts nicht geschlossen werden. Ich habe angeregt, falls die Schwangerenberatung nicht in andere Räume verlegt werden kann, zumindest geeignete Schutzmaßnahmen, z. B. das Anbringen blickdichter Gardinen, zu ergreifen.

- Weiterhin habe ich festgestellt, dass die bei der Schwangerenkonfliktberatung verwendeten Vordrucke „Beratungsbescheinigung“ und „Protokoll zur Schwangerenkonfliktberatung“ zwar getrennt voneinander aufbewahrt werden, jedoch Unsicherheiten hinsichtlich der Vernichtung der Unterlagen bestehen. Außerdem werden die Beratungsbeschei-

nigungen und die Protokolle in einfachen Holzschränken und jeweils in der Reihenfolge ihres Entstehens aufgehoben.

Hierzu habe ich der Gesundheitsabteilung mitgeteilt, dass gem. Art. 10 Abs. 2 Satz 2 BaySchwBerG die Beratungsbescheinigungen sorgfältig unter Verschluss zu halten und nach Ablauf von fünf Jahren zu vernichten sind. Die Beratungsprotokolle sind sorgfältig und getrennt von den Beratungsbescheinigungen unter Verschluss zu halten und nach Ablauf von drei Jahren zu vernichten, Art. 9 Abs. 1 BaySchwBerG.

Datenschutzrechtlich bedenklich ist die Aufbewahrung dieser Unterlagen in einfachen Holzschränken. Ich habe angeregt, diese Schränke durch Schränke mit Stahltüren bzw. Stahlschüben zu ersetzen. Bedenklich ist ferner die Aufbewahrung der Durchschriften der Beratungsbescheinigungen und der Protokolle in chronologischer Reihenfolge, da diese nachträglich zusammengeführt werden können und sich aus der Beratungsbescheinigung bei nicht anonymer Beratung der Name der beratenen Frau ergibt. Es muss daher regelmäßig umsortiert werden.

- Die Gesundheitsabteilung führt eine eigene - vom Landratsamt unabhängige - Registratur. Diese eigenständige Registratur ist aus datenschutzrechtlicher Sicht unbedingt notwendig. Hierzu weise ich auf die Begründung zum Entwurf des Gesetzes für die Eingliederung der staatlichen Gesundheitsämter und der staatlichen Veterinärämter in die Landratsämter (Landtagsdrucksache 13/2890, Seite 9) hin.
- Weiterhin habe ich festgestellt, dass sich die Akten der Gesundheitsabteilung in den jeweiligen Sachgebieten bzw. bei den zuständigen Sacharbeitern befinden. Sie werden bei Bedarf mit Hilfe der Zentralkartei zusammengeführt. Die Akten aus der freiwilligen gesundheitlichen Beratung und Begutachtung werden in jedem Fall getrennt von den übrigen Aktenbeständen der Gesundheitsabteilung geführt.

  Unterlagen der Gesundheitsabteilung über die selbe Person aus freiwilliger Beratung oder Begutachtung einerseits und hoheitlicher Tätigkeit andererseits dürfen nicht in einer Einheitsakte geführt werden, weil sonst beim Ziehen der Akte zum Vollzug hoheitlicher Maßnahmen die durch Art. 6 GDG besonders geschützten vertraulichen Angaben zur Kenntnis

genommen würden (vgl. 17. TB, Nr. 3.5.1, Ziffer 1 und Seite 26, 2. Spiegelstrich). Es hat also eine strikte Trennung der Akten aus dem Bereich der freiwilligen gesundheitlichen Beratung und Begutachtung von den übrigen Aktenbeständen der Gesundheitsabteilung zu erfolgen. In der geprüften Gesundheitsabteilung war diese Trennung gewährleistet.

- Auch die Ausgestaltung der Zentralkartei stieß auf keine datenschutzrechtlichen Bedenken. Diese Zentralkartei wird als reine Suchkartei auf weißen Karteikarten geführt, die alphabetisch geordnet sind. Darauf vermerkt sind der Name, der Vorname und das Geburtsdatum des Betroffenen und ein Hinweis, wegen welcher Vorgänge jemand im Amt war. Die Vorgänge sind dann im jeweiligen Sachgebiet zu finden. Die Suchkartei enthält keine Hinweise auf Vorgänge einer freiwilligen Beratung, so dass ein Zusammenführen der Unterlagen nur möglich ist, wenn der Betroffene einen Hinweis gibt.

  Die Zentralkartei darf keine inhaltlichen Hinweise auf bestimmte Erkrankungen oder persönliche Lebensumstände neben den notwendigen Suchmerkmalen enthalten, wenn damit Informationen aus der freiwilligen Beratung an andere Tätigkeitsbereiche der Gesundheitsabteilung gelangen können (vgl. 10. TB, Nr. 2.3.1 und 11. TB, Nr. 2.2). Zumindest die Unterlagen über Beratung und Begutachtung müssen im jeweiligen Sachgebiet verbleiben. Die Aufgabe einer Suchkartei kann auch damit erfüllt werden, dass nur formale Hinweise darauf aufgenommen werden, in welchen Sachgebieten Vorgänge zu der betreffenden Person vorhanden sind. Aus der Angabe eines bestimmten Sachgebiets dürfen jedoch keine Rückschlüsse auf bestimmte Erkrankungen möglich sein, die bei freiwilliger Beratung/Begutachtung angesprochen worden sind. Dies kann z. B. der Fall sein, wenn diesem Sachgebiet nur bestimmte Krankheiten zugewiesen sind (vgl. 15. TB, Nr. 2.4).

- Ferner habe ich bei der Prüfung festgestellt, dass in der Gesundheitsabteilung gegenwärtig keine automatisierte Datenverarbeitung benutzt wird. Computer werden nur zur Textverarbeitung verwendet. Wegen des zukünftig beabsichtigten Einsatzes der automatisierten Datenverarbeitung habe ich darauf hingewiesen, dass dieselben Grundsätze wie bei einer Zentraldatei gelten. Das DV-System darf keine Angaben über gesundheitliche Probleme, die die Gesundheitsabteilung bei freiwilliger Beratung oder Begutachtung erfahren hat, für die Sachbearbeitung außerhalb dieser Tätigkeit zur Verfügung stellen (vgl. hierzu 15. TB,

Nr. 2.4). Dies gilt sowohl intern in der Gesundheitsabteilung als auch gegenüber den anderen Abteilungen des Landratsamts. Die Art der Erkrankung, die bei freiwilliger Beratung oder Begutachtung bekannt wurde, darf am Bildschirm nur dem für diese freiwillige Beratung und Begutachtung zuständigen Mitarbeiter angezeigt werden. Zulässig ist die Anzeige der Nummern der Sachgebiete, die sich in freiwilliger Beratung oder Begutachtung mit dem Besucher befasst haben, solange die Sachgebietsnummern so vergeben sind, dass sie nicht auf ein bestimmtes gesundheitliches Problem hinweisen.

- Hinsichtlich der Organisation des Posteinlaufs habe ich zunächst auf meinen 17. TB (Nr. 3.5.1, Ziffer 5 und 1. Spiegelstrich) verwiesen. Ergänzend war zu bemerken, dass den Ratsuchenden empfohlen werden könnte, auf ihren Sendungen geeignete Zusätze anzubringen. Ein entsprechender Hinweis auf die Kenntlichmachung „sensibler Briefe“ (z.B. durch „persönlich“, „Schwangerenberatung“ etc.) könnte auch gut sichtbar in der Dienststelle angeschlagen werden.

  Im Rahmen der Prüfung habe ich zudem festgestellt, dass der Posteinlauf über die Poststelle des Landratsamts gem. § 15 der dortigen Geschäftsordnung erfolgt. Von der Haupt- und Personalverwaltung des Landratsamts wurden die Bediensteten der Poststelle mündlich angewiesen, dass als Arztbefunde bzw. –schreiben an die Schwangerenberatungstelle oder die Aidsberatung erkenntliche Sendungen ungeöffnet an die Gesundheitsabteilung weitergeleitet werden müssen. In der Gesundheitsabteilung wird der Posteinlauf in ein Posteingangsbuch eingetragen und an den für die Bearbeitung Zuständigen weitergeleitet.
  Ich habe darauf hingewiesen, dass die oben dargestellten Maßgaben des 17. TB, die den Landratsämtern vom Staatsministerium des Innern im Schreiben vom 07.12.1995 mitgeteilt wurden, den Bediensteten der Poststelle nicht nur mündlich sondern auch schriftlich bekannt zu geben sind. Ggf. bietet sich auch das Erstellen einer Dienstanweisung an. § 15 der Geschäftsordnung des Landratsamts aus dem Jahre 1989 war immer noch auf den Eingang „normaler“ Behördenpost in einem Landratsamt ohne Gesundheitsabteilung zugeschnitten und berücksichtigte nicht die besondere Tätigkeit einer Gesundheitsabteilung.

  Wegen Fragen der Abschottung von Datenbeständen der Gesundheitsabteilung bei zentraler EDV verweise ich auf Nr. 17.3.6 dieses Berichts.

3.9 Weitergabe von Erkenntnissen aus Heilfürsorgeunterlagen

Eine Polizeibeamtin hat mir vorgetragen, dass ein Polizeiarzt Erkenntnisse aus ihrer Behandlung im Rahmen der freien Heilfürsorge an ihren Dienstvorgesetzten weitergegeben habe, obwohl weder ihre Einwilligung noch ein Gutachtensauftrag des Dienstherrn vorlag. Ich habe das wie folgt beurteilt:

Den Beamten der Bayerischen Bereitschaftspolizei, die aufgrund dienstlicher Verpflichtung in einer Gemeinschaftsunterkunft wohnen, wird freie Heilfürsorge gewährt. Dies bedeutet, dass die Beamten im Regelfall durch den Polizeiärztlichen Dienst ärztlich versorgt werden. Tritt ein Polizeiarzt in der Funktion eines behandelnden Arztes im Rahmen der freien Heilfürsorge auf, unterliegen daher die hierbei entstehenden Unterlagen und Erkenntnisse in vollem Umfang der ärztlichen Schweigepflicht (§ 203 StGB). Anders als im Fall einer im Auftrag des Dienstherrn vorzunehmenden ärztlichen Begutachtung (z.B. Dienstunfähigkeitsuntersuchungen) darf der Arzt Untersuchungsergebnisse aus der freien Heilfürsorge nicht ohne Befugnis (z.B. Einwilligung des Betroffenen) an Dritte weitergeben.

Eine Durchbrechung der ärztlichen Schweigepflicht wäre dann gerechtfertigt gewesen, wenn die Beamtin wegen der angenommenen Beeinträchtigung ihrer Gesundheit in ihrer konkreten dienstlichen Funktion eine akute Gefahr für sich selbst oder andere Personen dargestellt hätte. Eine solche akute Gefahrenlage konnte vom Dienstherrn nicht dargelegt werden. Ich habe daher die Datenweitergabe durch den Polizeiärztlichen Dienst förmlich beanstandet.

Das Präsidium der Bayer. Bereitschaftspolizei hat daraufhin eine Arbeitsgruppe eingesetzt, die sich mit der Erstellung von Leitlinien zur ärztlichen Schweigepflicht für den Polizeiärztlichen Dienst befasst, um den betroffenen Medizinern eine Entscheidungshilfe an die Hand zu geben. Darüber hinaus habe ich im Zusammenhang mit der datenschutzrechtlichen Prüfung eines Polizeiärztlichen Dienstes erreicht, dass künftig zur bereits bestehenden personellen Trennung zwischen dem Bereich der Heilfürsorge und den übrigen Funktionen im Polizeiärztlichen Dienst auch eine organisatorische Trennung der Akten vorgenommen wird.

3.10 Unzulässige Verarbeitung von Daten Behinderter in einem Universitätsinstitut

Wie mir durch Presseartikel bekannt wurde, verarbeitete das Humangenetische Institut einer bayerischen Universität personenbezogene Daten und Blutproben von Bewohnern eines nicht meiner Kontrollbefugnis unterliegenden Behindertenwohnheims. Die ehemalige Leiterin des Medizinischen Dienstes dieses Wohnheims hatte die Patientendaten und Blutproben an das Institut weitergegeben, ohne eine Einwilligung der Betroffenen bzw. ihrer Betreuer (gesetzlichen Vertreter) einzuholen. Die Daten wurden auch in einer Dissertation einer Doktorandin des Instituts verwertet.

Ich habe diesen Vorgang beanstandet und meine Beanstandung vor allem damit begründet, dass personenbezogene Daten von Heimbewohnern ohne Einwilligung der Betroffenen bzw. ihrer gesetzlichen Vertreter oder eine andere Offenbarungsbefugnis, das heißt rechtswidrig an das Humangenetische Institut übermittelt wurden. Daher durften sie dort auch nicht verarbeitet, insbesondere gespeichert oder genutzt werden. Aus der Unzulässigkeit der Übermittlung an das Institut folgt die Unzulässigkeit einer weiteren Verarbeitung durch dieses. Auch Art. 27 Abs. 4 des Bayerischen Krankenhausgesetzes (BayKrG) bietet keine Rechtsgrundlage für diese Vorgehensweise, da diese Vorschrift rechtmäßig erhobene Daten voraussetzt. Ich habe klargestellt, dass es nicht darauf ankommt, ob die Mitarbeiter des Instituts darauf vertrauen durften, dass von Seiten des Medizinischen Dienstes des Wohnheims die zur zulässigen Offenbarung erforderlichen Einwilligungen eingeholt wurden. Entscheidend war, dass die Patientendaten ohne Befugnis übermittelt wurden und diese rechtswidrige Übermittlung zur Rechtswidrigkeit der weiteren Verarbeitung und Nutzung dieser Daten führt.

Ich konnte mich auch nicht der Auffassung des Instituts anschließen, dass die Auswertung der Blutproben zu genetischen Untersuchungen unter einen kurativen Auftrag des Medizinischen Dienstes fällt. Zwar enthält § 1 des Heimvertrags die Klausel „Versorgung unter Wahrung des Rechts auf freie Arztwahl“. Eine Einwilligung in eine genetische Untersuchung kann ich hierin jedoch nicht sehen, da es sich hier allenfalls um eine Einwilligung zu den erforderlichen Untersuchungen durch den Medizinischen Dienst des Heims handelt. Auch eine mutmaßliche Einwil-

ligung in eine genetische Untersuchung kann nicht unterstellt werden, da damit weder die Behinderten noch ihre gesetzlichen Vertreter zu rechnen brauchen.

4 Sozialbehörden

4.1 Presse- und Öffentlichkeitsarbeit mit Sozialdaten

Wie sich im Berichtszeitraum gezeigt hat, geben **Ausländerbehörden** bei ihrer Presse- und Öffentlichkeitsarbeit gelegentlich **Sozialdaten** bekannt, die sie bspw. vom Sozialamt zur Bearbeitung und Entscheidung ausländerrechtlicher Verwaltungsvorgänge erhalten haben. Das Sozialamt übermittelt den Ausländerbehörden für die Entscheidung über den Aufenthalt eines Ausländers nach § 71 Abs. 2 SGB X Daten über die Gewährung von Sozialhilfeleistungen.

Aus gegebenem Anlass empfehle ich den Sozialleistungsträgern, die Ausländerbehörden (und zweckmäßiger Weise auch andere Nicht-SGB-Stellen) in geeigneter Form auf die Zweckbindung und Geheimhaltungspflicht der Empfänger von Sozialdaten nach § 78 SGB X hinzuweisen.

Besondere Vorsicht im Umgang mit Sozialdaten ist bei der Presse- und Öffentlichkeitsarbeit geboten:

Nicht-SGB-Stellen wie etwa Ausländerbehörden sind nämlich nach § 78 Abs. 1 S. 1 und 2 SGB-X bei ihrer Presse- und Öffentlichkeitsarbeit zur Bekanntgabe von Sozialdaten nur insoweit berechtigt als auch die Sozialbehörde, die die Sozialdaten übermittelt hat, selbst Öffentlichkeitsarbeit damit betreiben dürfte. Die Voraussetzungen der Zulässigkeit einer Veröffentlichung von Angaben über die Erbringung von Sozialleistungen hat der Gesetzgeber in § 69 Abs. 1 Nr. 3 SGB X konkret und abschließend geregelt. Presse- und Öffentlichkeitsarbeit unter Verwendung solcher Sozialdaten ist danach nur zulässig, soweit sie erforderlich ist für die **Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen** im Zusammenhang mit einem Verfahren über die Erbringung von Sozialleistungen; die Übermittlung bedarf der vorherigen Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde.

Auf die nach § 69 Abs. 1 Nr. 3 SGB X erforderliche, vor der Veröffentlichung einzuholende ministerielle Genehmigung kann auch dann nicht verzichtet werden, wenn die betroffene Stelle von einer Anfrage der Medien überrascht wird. Eine Prognose, wonach die ministerielle Genehmigung wohl schon erteilt werden würde bzw. müsste, ist nämlich keineswegs immer zutreffend.

Vor allem aber zielt § 69 Abs. 1 Nr. 3 SGB X mit dem Erfordernis einer **vorherigen** Genehmigung der Veröffentlichung darauf ab, dass eine **mit der betroffenen Stelle nicht identische Behörde** überprüft, ob die beabsichtigte Veröffentlichung von Sozialdaten dem Grunde und dem Umfang nach angemessen bzw. verhältnismäßig ist. Die Genehmigungsbehörde hat nicht zuletzt darauf zu achten, dass persönliche Gesichtspunkte keinen unangemessenen Einfluss auf die Übermittlungsabsicht der betroffenen Behörde erlangen.

Keinesfalls darf die Behörde von einer Einwilligung des Betroffenen in die Veröffentlichung von Sozialdaten ausgehen, wenn die Voraussetzungen nach § 69 Abs. 1 Nr. 3 SGB X nicht vorliegen. Dies gilt auch dann, wenn die öffentliche Diskussion etwa einer Ausweisung von der betroffenen Familie selbst oder in deren Auftrag von einer Interessenvertretung herbeigeführt wurde. An der Bekanntgabe der im Zusammenhang mit Ausweisungen vielfach relevanten Informationen über erbrachte Sozialleistungen wie etwa der Dauer und Gesamthöhe bezogener Sozialhilfeleistungen und an deren Diskussion haben die Betroffenen nämlich in der Regel gerade kein Interesse.

Zur datenschutzrechtlichen Problematik behördlicher Presse- und Öffentlichkeitsarbeit habe ich mich in diesem Tätigkeitsbericht auch unter der Rubrik „Medien“, Ziffer 16.1 (Fall „Mehmet“) eingehend geäußert; auf die dortigen Ausführungen möchte ich an dieser Stelle ausdrücklich hinweisen.

4.2 Gesetzliche Krankenversicherung

4.2.1 Gesetz zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000

Der Gesetzentwurf zur GKV-Gesundheitsreform 2000 enthielt u.a. Neuregelungen bzw. Änderungen mit teilweise ganz erheblichen Auswirkungen auf das Recht auf informationelle Selbstbestimmung der gesetzlich Krankenversicherten. Die Darstellung aller datenschutzrechtlichen Regelungen, zu denen ich mich gegenüber dem Bayerischen Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit und im Kreise der Datenschutzbeauftragten geäußert habe, würde allerdings den angemessenen Umfang dieses Beitrags überschreiten. Ich beschränke meine Berichterstattung deshalb auf die wesentlichsten Punkte und verweise hierzu auch auf die als Anlagen 6 und 10 dieses Tätigkeitsberichts abgedruckten Entschließungen der Datenschutzbeauftragten des Bundes und der Länder vom 25.08.1999 und vom 07./08.10.1999 sowie auf den als Anlage 7 abgedruckten Appell von Datenschutzbeauftragten des Bundes und der Länder vom 24.11.1999.

Die zentrale datenschutzrechtlich bedeutsame Zielsetzung des Gesetzentwurfs war die Verbesserung der Datentransparenz und der Datengrundlagen zur Steuerung des Leistungs- und Ausgabengeschehens der gesetzlichen Krankenversicherung und für die Gesundheitsberichterstattung des Bundes und der Länder. Hierzu sollten eine verbesserte Bereitstellung steuerungsrelevanter Daten durch sog. Datenannahmestellen erreicht und die kassenartenübergreifende Datenzusammenführung durch Arbeitsgemeinschaften der Krankenkassen bzw. ihrer Verbände vorgeschrieben werden. In diesem Zusammenhang sah der ursprüngliche Gesetzentwurf die versichertenbezogene Übermittlung aller Abrechnungsdaten aller Leistungserbringer mit medizinischen Inhalten und Diagnosedaten an die Krankenkassen vor. Im Gegensatz zum bisherigen Verfahren sollten somit auch medizinische Abrechnungsdaten aus der ambulanten Versorgung versichertenbezogen zur Kenntnis der Krankenkassen gelangen. Damit wäre bei den gesetzlichen Krankenkassen über jeden Versicherten personenbezogen eine vollständige Behandlungs- und Verordnungsdatensammlung und ein lückenloses Profil seines Gesundheitszustands entstanden, ohne dass dies zur Steuerung im GKV-System und für die Gesundheitsberichterstattung tatsächlich erforderlich gewesen wäre. Die Ziele der Reform lassen sich auch erreichen, wenn die Krankenkassen die medizinischen Abrechnungsdaten aus allen Leistungsbereichen nicht versichertenbezogen,

sondern in pseudonymisierter Form auswerten und die Identifizierung der Versicherten nur zur Erfüllung gesetzlich festgelegter Aufgaben der Krankenkassen und Kassen(zahn)ärztlichen Vereinigungen zugelassen und ermöglicht wird. Der Ausschuss für Gesundheit im Deutschen Bundestag entsprach sogar dem Vorschlag der Datenschutzbeauftragten, die Pseudonymisierung der Versicherten auch hinsichtlich der Abrechnungen der Krankenhäuser, nichtärztlicher Leistungserbringer und Apotheken vorzuschreiben, deren Abrechnungsdaten bisher versichertenbezogen bei der Krankenkasse gespeichert werden. Eine solche umfassende Pseudonymisierung der Versichertendaten gegenüber den Krankenkassen sollte bei den sog. Datenannahmestellen vorgenommen werden, zu deren Bildung die Spitzenverbände der Krankenkassen nach dem Gesetzentwurf ohnehin verpflichtet werden sollten.

Die Datenannahmestellen, die räumlich, organisatorisch und personell von den Krankenkassen und ihren Verbänden hätten getrennt werden müssen, sollten die ihnen von den Leistungserbringern übermittelten Abrechnungsdaten auf sachliche Richtigkeit und Rechtmäßigkeit der Leistungsabrechnung sowie hinsichtlich der Zuständigkeit der Krankenkassen für die jeweiligen Versicherten prüfen. Anschließend sollten die Datenannahmestellen die hinsichtlich der Versicherten pseudonymisierten Abrechnungsdaten den zuständigen einzelnen Krankenkassen und desweiteren den jeweiligen auf Landesebene zu bildenden „Arbeitsgemeinschaften zur Datenaufbereitung“ übermitteln. Aufgaben dieser Arbeitsgemeinschaften sollten die Zusammenführung der übermittelten Abrechnungsdaten und deren Aufbereitung sein, u.a. für Zwecke der Wirtschaftlichkeits- und Qualitätsprüfungen, der Vereinbarung der Arznei-, Verband- und Heilmittelbudgets und für Steuerungsaufgaben der Krankenkassen(-verbände), der Kassen(zahn)ärztlichen Vereinigungen und der Landeskrankenhausgesellschaften im Rahmen der Bedarfs- und Versorgungsplanung sowie der Vertragsvorbereitung und –durchführung zur Vergütung der Leistungserbringer.

Der im Sinne der datenschutzrechtlichen Forderungen wesentlich verbesserte Gesetzentwurf wurde zwar vom Bundestag beschlossen, dann aber – und zwar nicht wegen seiner datenschutzrechtlichen Komponenten, sondern wegen anderweitiger gesundheitspolitischer Erwägungen - vom Bundesrat abgelehnt. Der Appell von Datenschutzbeauftragten des Bundes und der Länder, die zustimmungspflichtigen versicherten- und datenschutzfreundlichen Gesetzesteile in den Bundesrat einzubringen und dass der Bundesrat diesen Regelungen zustimmen solle, blieb leider

ohne Erfolg. Weder wurden diese bedeutsamen datenschutzrechtlichen Verbesserungen seinerzeit in einem gesonderten Gesetz zur Verbesserung des Datenschutzes und der Datengrundlagen der gesetzlichen Krankenkassen zusammengefasst, noch sind sie in der schließlich zum 01.01.2000 in Kraft getretenen Fassung des GKV-Gesundheitsreformgesetzes 2000 enthalten.

Das Bundesministerium für Gesundheit hat jedoch in Aussicht gestellt, datenschutzfreundliche Veränderungen der Datenerhebungs-, -verarbeitungs- und -nutzungsregelungen im Recht der gesetzlichen Krankenversicherung weiter zu verfolgen.

4.2.2 Übermittlung von Sozialdaten an das Gericht in Unterhaltsverfahren (§ 74 SGB X)

Gem. § 74 S.1 Ziff. 1 a SGB X ist die Übermittlung von Sozialdaten durch einen Sozialleistungs- oder Sozialversicherungsträger wie bspw. eine Krankenkasse zulässig, soweit diese Übermittlung für die Durchführung eines gerichtlichen Verfahrens wegen eines gesetzlichen oder vertraglichen Unterhaltsanspruchs erforderlich ist.

In einem von mir untersuchten Fall hatte ein Amtsgericht im Verfahren gegen den Versicherten wegen Unterhalts für die geschiedene Ehefrau die Krankenkasse aufgefordert, dem Gericht „Auskunft zu erteilen über die Höhe der Einkünfte des Beklagten im Jahre 1998“. Daraufhin übersandte die Krankenkasse den vollständigen Einkommensteuer-Bescheid betreffend den beklagten Versicherten und dessen zweite Ehefrau in Fotokopie an das Gericht. Auf diesem Einkommensteuer-Bescheid waren keinerlei Angaben geschwärzt.

In meiner datenschutzrechtlichen Bewertung habe ich die Krankenkasse darauf hingewiesen, dass das Amtsgericht lediglich nach der Höhe der **Einkünfte des Beklagten** gefragt, nicht aber um Auskunft betreffend die zweite Ehefrau des Beklagten ersucht hatte. Bereits insoweit war die erteilte Auskunft durch die Krankenkasse an das Amtsgericht nicht erforderlich und daher unzulässig.
Aber auch hinsichtlich der Daten des beklagten Versicherten war die Übersendung des vollständigen Einkommensteuer-Bescheids an das Amtsgericht inhaltlich zu weitgehend. Zwar kann nach § 74 S. 1 Ziff. 1 a SGB X für gerichtliche Unterhaltsverfahren grundsätzlich auch die Über-

sendung vollständiger Einkommensteuer-Bescheide zulässig sein. Da die Verantwortung für die Zulässigkeit einer solchen Datenübermittlung gem. § 67 d Abs. 2 S. 1 SGB X aber bei der SGB-Stelle liegt, muss **diese** überprüfen (können), inwieweit die Angaben im Einkommensteuer-Bescheid für das Unterhaltsverfahren erforderlich sind. Die SGB-Stelle muss diese Überprüfung anhand der Formulierung des Auskunftsersuchens des Gerichts vornehmen und hat dabei den Wortlaut des gerichtlichen Auskunftsersuchens strikt zu beachten.

Vorliegend war also nach der Höhe der **Einkünfte des Beklagten** gefragt, nicht etwa nach dessen zu versteuerndem Einkommen, schon gar nicht nach dem infolge gemeinsamer Veranlagung zu versteuernden Einkommen, das sich im Einkommensteuer-Bescheid u.a. aus Betragsangaben errechnet, in denen Werte für beide Ehegatten zusammengefasst sind, ohne dass der Anteil des Beklagten daraus entnommen werden könnte. Aufgrund der gerichtlichen Anfrage hätten dem Amtsgericht auf der Grundlage des Einkommensteuer-Bescheids lediglich die den Petenten betreffenden Einkünfte aus nichtselbstständiger bzw. selbstständiger Tätigkeit sowie aus Vermietung und Verpachtung nebst Gesamtbetrag seiner Einkünfte mitgeteilt werden dürfen. Soweit sich der Krankenkasse Zweifel über den Umfang des gerichtlichen Auskunftsersuchens aufgedrängt haben sollten, hätten diese mit dem Amtsgericht geklärt werden müssen, dessen Auskunftsersuchen die maßgebliche Telefonnummer nebst Nebenstelle enthielt.

Ich habe die Krankenkasse wegen der dargelegten Datenschutzverstöße beanstandet. Sie betrafen sensible Daten, die in der Finanzverwaltung durch das Steuergeheimnis geschützt sind. Auch lag nicht etwa eine gemeinsame Veranlagung des beklagten Versicherten mit der Klägerin vor, so dass durch die Datenschutzverletzung für die Unterhaltsklage gegen den Eingabeführer Daten an das Gericht übermittelt worden wären, die lediglich auch die finanziellen und steuerlichen Verhältnisse der Klägerin selbst geoffenbart hätten. Vielmehr wurden der Klägerin durch das Fehlverhalten der Krankenkasse die Einkünfte der zweiten Ehefrau des Beklagten zugänglich, u.a. weil die Klägerin beim Amtsgericht Akteneinsicht in die Gerichtsakten über das Unterhaltsverfahren nehmen konnte.

4.3 Medizinischer Dienst der Krankenversicherung (MDK)

4.3.1 Verpflichtung von (Zahn-)Ärzten zur Übersendung von Behandlungsunterlagen an den MDK

Soweit die Krankenkassen nach § 275 Abs. 1 bis 3 SGB V eine gutachtliche Stellungnahme oder Prüfung durch den MDK veranlasst haben, sind die Leistungserbringer, also insbesondere (Zahn-)Ärzte nach § 276 Abs. 2 S. 1 2. Hs. SGB V verpflichtet, „**Sozialdaten**“ auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist. Die Kassenzahnärztliche Vereinigung Bayerns (KZVB) bat mich um datenschutzrechtliche Bewertung, was in diesem Zusammenhang unter dem Begriff „Sozialdaten“ zu verstehen sei. Hintergrund der Anfrage war, dass der MDK und Krankenkassen darunter auch Behandlungsunterlagen wie bspw. Röntgenaufnahmen, Zahnmodelle, Karten aus der Patientenkartei des (Zahn-)Arztes usw. rechnen.

Gemäß § 67 Abs. 1 S. 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden. Darunter fallen auch Patientendaten. Dies gilt unabhängig davon, ob solche Einzelangaben auf einem Datenträger wie z. B. einer Karteikarte, einem Zahnabdruck, einem Röntgenbild, Röntgen-CT oder einer Kernspinaufnahme gespeichert sind oder aber in einem ärztlichen Bericht oder Gutachten.

Laut Gesetzesbegründung zu § 276 Abs. 2 S. 1 2. Hs. SGB V sieht der Gesetzgeber darin „auch eine Rechtsgrundlage für die Übermittlung des Krankenhausentlassungsberichts an den Medizinischen Dienst, soweit erforderlich“. Daraus lässt sich ableiten, dass der Gesetzgeber davon ausgeht, dass der Begriff „Sozialdaten“ insoweit durchaus auch Behandlungsunterlagen umfassen kann und für den MDK nicht etwa nur mündliche oder speziell zu dieser Auskunftserteilung neu verfasste schriftliche Auskünfte als erforderlich in Betracht kommen können.

„Sozialdaten“ i.S.d. § 276 Abs. 2 S. 1 2. Hs. SGB V umfassen damit **grundsätzlich alle** die Behandlung eines Patienten betreffenden Auskünfte **und Unterlagen** einschließlich bspw. solcher

über Befunde und einschließlich angefertigter Röntgenaufnahmen etc., soweit solche Angaben bzw. Unterlagen – wiederum grundsätzlich – für die gutachtliche Stellungnahme und Prüfung durch den MDK als erforderlich in Betracht kommen.

Davon zu unterscheiden ist die Frage, welche „Sozialdaten“ nach dieser Vorschrift **im konkreten Einzelfall** und gemessen am **konkreten Prüfungsauftrag**, den der MDK von der Krankenkasse erhalten hat, an diesen übermittelt werden müssen, weil sie für diese **konkrete** gutachtliche Stellungnahme und Prüfung als erforderlich anzusehen sind. Im konkreten Einzelfall erstreckt sich die Auskunftsverpflichtung der Leistungserbringer nach § 276 Abs. 2 S. 1 2. Hs. SGB V deshalb keineswegs immer auf **alle** die Patientenbehandlung betreffenden Unterlagen.

4.4 Kassenärztliche Vereinigung Bayerns (KVB)

4.4.1 Weitergabe laborärztlicher Abrechnungsdaten an ärztliche Sachverständige zur Abrechnungsüberprüfung

Aufgrund erheblicher jährlicher Leistungsausweitung und erheblicher Kosten zur Punktwertstützung hatte der KVB-Vorstand eine Vorstandsarbeitsgruppe zur Analyse und zur Mengenbegrenzung im O-III Laborbereich eingesetzt. O III-Laborleistungen sind spezielle Laborleistungen, die nur Ärzte mit besonderer Qualifikation und aufgrund einer Genehmigung der KV erbringen dürfen. O III-Laborleistungen werden nicht vom auftraggebenden Arzt, sondern vom Laborarzt mit der KV abgerechnet. Mitglieder der genannten Arbeitsgruppe waren Funktionsträger der KVB sowie Mitarbeiter der KVB-Verwaltung. Die Arbeitsgruppe beabsichtigte seinerzeit eine Überprüfung der Abrechnungen von Laborärzten aus den Quartalen IV/1996 und II/1997. Überprüft werden sollten die Abrechnungen der Laborärzte, deren Abrechnungswerte 20% und mehr über dem Durchschnitt lagen, später auch der Ärzte, deren Abrechnungswerte den Durchschnitt um 5% und mehr überschritten. Die KVB-Vorstandsarbeitsgruppe berief als ärztlichen Sachverständigen zur Durchführung der Abrechnungsprüfungen neben anderen Laborärzten einen bestimmten namhaften bayerischen Laborarzt. Die Untersuchungsergebnisse der Sachverständigen sollten anschließend von der Vorstandsarbeitsgruppe bewertet und mit Vorschlägen über Maßnahmen der KVB verbunden werden.

Im Verlauf des Abrechnungsprüfungsverfahrens wurde dem besagten Sachverständigen nun aber auch eine Liste mit Abrechnungsdaten eines Quartals übermittelt, das nicht in die Prüfung einbezogen werden sollte. Außerdem enthielt diese Liste Abrechnungsdaten von wesentlich mehr Ärzten als von der Vorstandsarbeitsgruppe zur Prüfung ausgewählt worden waren. Der besagte Prüfarzt, der mit anderen Laborärzten in einem erheblichen Konkurrenzverhältnis steht, erhielt dadurch Kenntnis von den Einkommensverhältnissen und Praxisumständen der Konkurrenten in einem Ausmaß, das durch die Prüfung nicht gerechtfertigt war. Diese Datenübermittlung stellt einen erheblichen Verstoß gegen das Recht der anderen Ärzte auf vertrauliche Behandlung ihrer Praxisumstände durch die KVB und damit gegen den Datenschutz dar.

Des Weiteren hatte die KVB diesem Prüfarzt einen elektronischen Datenträger mit Abrechnungsdaten eines anderen Laborarztes in der Form zur Verfügung gestellt, dass der Sachverständige die Möglichkeit hatte, die Daten in seinen eigenen Räumen und mit seiner eigenen EDV auszuwerten. Die KVB hatte somit die notwendigen organisatorischen Sicherungsmaßnahmen unterlassen, weil sie durch diese Form der Datenweitergabe die Kontrolle über die Auswertung des sensiblen Abrechnungsdatenbestandes zumindest zeitweilig völlig aus der Hand gegeben hatte.

Es liegt mir fern, angemessene Prüfungen durch die KVB zu behindern. Datenübermittlungen müssen sich aber im Rahmen dessen halten, was für die Prüfung erforderlich ist. Auch müssen die Grundsätze ordnungsgemäßer technischer und organisatorischer Sicherungsmaßnahmen eingehalten werden. Dies war vorliegend nicht der Fall. Ich habe die KVB daher wegen unzulässiger Datenweitergabe an diesen Sachverständigen im Rahmen der Prüfung von Laborarztabrechnungen förmlich beanstandet.

Inwieweit ein unmittelbarer Konkurrent als Sachverständiger in die Abrechnungsprüfung eingeschaltet werden darf, stellt eine fachlich zu überprüfende und zu entscheidende Frage dar, die über meinen Prüfungsmaßstab von datenschutzrechtlichen Vorschriften hinausgeht. Hierbei handelt es sich um eine von der Selbstverwaltungskörperschaft KVB und ggf. von der Rechtsaufsichtsbehörde zu entscheidende Fachfrage. Ich habe die KVB aufgefordert, die Voraussetzungen und Modalitäten einer Bestellung der Mitglieder und ärztlichen Sachverständigen von Vorstandsarbeitsgruppen, -referaten und -kommissionen sowie -ausschüssen zur Unterstützung des Vorstands bei der Erfüllung seiner gesetzlichen und satzungsmäßigen Aufgaben in der KVB-Satzung zu regeln. Solche Mitglieder und Sachverständige sind förmlich auf die gewissenhafte Erfüllung ihrer Obliegenheiten einschließlich der Einhaltung datenschutzrechtlicher Bestimmungen zu verpflichten. Die Frage, ob eine bestimmte Person aufgrund gesetzlicher Bestimmungen von der vorgesehenen Tätigkeit möglicherweise ausgeschlossen ist, muss vor der Bestellung seitens der KVB im Einzelfall und im Zweifel durch die Rechtsaufsicht geprüft werden.

Noch nicht abgeschlossen ist meine datenschutzrechtliche Kontrolle der KVB hinsichtlich der Frage, ob durch Auslage in den Sitzungen der Vorstandsarbeitsgruppe den Sachverständigen ebenfalls eine (andere) Liste mit Abrechnungsdaten von Laborärzten, die von der Abrechnungs-

prüfung nicht betroffen waren, zur Verfügung stand. Eine Überlassung dieser Liste an die Sachverständigen wäre in gleicher Weise unzulässig wie die Überlassung der o.g. Liste. Da die maßgeblichen Entscheidungen über die Einbeziehung auffälliger Laborärzte in die Abrechnungsprüfung nicht von den Sachverständigen, sondern von den Mitgliedern des Vorstandsreferats zu treffen sind, ist es nicht erforderlich und damit unzulässig, den Sachverständigen Abrechnungswerte auch zahlreicher anderer Ärzte offen zu legen, die keiner Prüfung unterzogen werden brauchten.

4.4.2 Lieferung von Rezeptdaten an die KVB

Die VSA Verrechnungsstelle der Süddeutschen Apotheken GmbH nimmt für Apotheken in Bayern deren Arzneimittelabrechnungen gegenüber den Krankenkassen vor. Vor kurzem beabsichtigte die KVB nun mit der VSA eine Vereinbarung über die Lieferung von Verordnungsdaten der bayerischen Vertragsärzte zu schließen. Danach sollten der KVB vor dem Hintergrund der gesetzlichen Budgetierung der Arzneimittelausgaben eine bis ins Kleinste detaillierte Analyse der vertragsärztlichen Rezeptverordnungen zur gezielten Information der bayerischen Vertragsärzte über deren Verordnungsverhalten und den Stand der Budgetausschöpfung ermöglicht werden. Die VSA sollte der KVB hierzu monatlich die Daten aller für die Mitgliedsapotheken der VSA abgerechneten und von bayerischen Vertragsärzten ausgestellten Rezepte versichertenbezogen auf Datenträgern zur Verfügung stellen.

Gegen den Umfang der vorgesehenen Datenlieferungen habe ich Einwände erhoben. Die Vereinbarung mit der VSA sah insbesondere eine Datenerhebung der KVB auch über die betroffenen Patienten vor. Dies hätte gegen § 285 Abs. 2 SGB V verstoßen. Nach dieser Vorschrift dürfen die KVen Einzelangaben über die persönlichen und sachlichen Verhältnisse der Versicherten nur erheben und speichern, soweit dies zur Durchführung von Wirtschaftlichkeits- und Qualitätsprüfungen (§§ 106 und 136 SGB V) sowie für Plausibilitätskontrollen und Auskünfte an Versicherte (§§ 83 Abs. 2, 305 SGB V) erforderlich ist. Eine entsprechende Regelung für die Beratung der Vertragsärzte fehlt. Hätte der Gesetzgeber den KVen für derartige Beratungen die Verwendung von **Versichertendaten** gestatten wollen, hätte er die Beratung nach § 305 a Abs. 2 SGB V in den Aufgabenkatalog des § 285 Abs. 2 SGB V aufgenommen bzw. aufnehmen müssen. Da dies nicht geschehen ist, darf die KVB für die beabsichtigte Beratung der Vertragsärzte

keine versichertenbezogenen Daten erheben und die VSA darf ihr dementsprechend keine versichertenbezogenen Rezeptdaten übermitteln. Auch § 84 Abs. 2 S. 1 SGB V sieht zur Beobachtung und Berechnung des Arzneimittelbudgets durch die KVen **keine** versichertenbezogene Erfassung der von den Vertragsärzten veranlassten Ausgaben bei Krankenkassen und KVen vor.

Die KVB hat mir inzwischen mitgeteilt, dass der genannte Vertrag mit der VSA in der bisherigen Entwurfsfassung nicht abgeschlossen werde. Die KVB werde mit der VSA nunmehr unter Einbeziehung der Krankenkassen weiter über Datenübermittlungen für Beratungen der Vertragsärzte durch die KVB nach § 305 a Abs. 2 SGB V verhandeln.

Jedenfalls die laut KVB wegen des Arzneimittelbudgets im Interesse der Vertragsärzte liegende sogenannte „Arzneikosten-Frühinformation“ lässt sich - wie mir die KVB mittlerweile bestätigt hat - auch aus weniger detaillierten Einzelangaben als bisher vorgesehen erstellen und vor allem ohne Kenntnis versichertenbezogener Rezeptdaten. Eine (nicht versichertenbezogene) monatliche Arzneikosten-Frühinformation der Vertragsärzte erachte ich wegen des Arzneimittelbudgets und ihnen drohender Regressmaßnahmen als grundsätzlich vom Sicherstellungsauftrag der KVB betreffend die vertragsärztliche Versorgung nach § 75 Abs. 1 S. 1 SGB V gedeckt. Eine angemessene, regelmäßige und rechtzeitige schriftliche Beratung der Ärzte in Form einer solchen „Frühinformation“ stellt gegenüber dem ihnen ggf. drohenden Regress bzw. gegenüber in Betracht kommenden Wirtschaftlichkeitsprüfungen den wesentlich geringeren Eingriff dar.

Hinsichtlich der (nicht versichertenbezogenen) Sozialdaten, die für angemessene Arzneikosten-Frühinformationen erforderlich sind, erachte ich die KVB auch als „berechtigte Stelle“ nach § 300 Abs. 2 S. 2 SGB V. Nach der genannten Vorschrift dürfen Apotheken-Rechenzentren die Daten für im SGB bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind. Die Beobachtung und Berechnung der Ausgaben betreffend das Arzneimittelbudget sowie rechtzeitige Informationen der Ärzte hierüber stellen solche im SGB vorgesehenen Aufgaben der KVB dar.

4.4.3 Auskünfte an Versicherte gemäß § 305 Abs. 1 S. 2 SGB V

§ 305 Abs. 1 S. 1 SGB V verpflichtet die **Krankenkassen**, die Versicherten auf deren Antrag über die im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und deren Kosten zu unterrichten. Damit dabei bei den Krankenkassen kein lückenloses Behandlungsprofil gesetzlich krankenversicherter Patienten entsteht („gläserner Patient"), haben die **Kassenärztlichen Vereinigungen** (KVen) den Krankenkassen nach § 305 Abs. 1 S. 2 SGB V bei solchen Auskünften die **Angaben über die von den Versicherten in Anspruch genommenen vertragsärztlichen Leistungen und deren Kosten** für jeden Versicherten **gesondert in einer Form zu übermitteln, die eine Kenntnisnahme durch die Krankenkasse ausschließt**. Die Krankenkassen haben die Angaben der KVen zusammen mit ihren eigenen Auskünften an den Versicherten weiterzuleiten. Diese gesetzlichen Anforderungen lassen sich ohne Schwierigkeiten dadurch umsetzen, dass die KVen die Patientendaten über die vertragsärztlichen Leistungen und deren Kosten in einen weiteren verschlossenen Umschlag legen und den Krankenkassen mit einem Hinweis wie etwa: „Patientendaten – Nur vom Versicherten zu öffnen!" zur Weiterleitung an den Auskunftsuchenden übersenden. Ohne § 305 Abs. 1 S. 2 SGB V würden derartige Auskunftsanträge der Versicherten den Krankenkassen Informationen der KVen über vertragsärztliche Leistungen zugänglich machen, deren Zuordnung zum einzelnen Patienten der Krankenkasse nur in bestimmten Fällen gestattet ist (bspw. zur Abrechnung von Erstattungsansprüchen gegenüber einem anderen Kostenträger).

Wie ich aufgrund einer Eingabe feststellen musste, verweigerte die KVB dem Beschwerdeführer, der über seine Krankenkasse Auskunft über die von ihm in Anspruch genommenen ärztlichen Leistungen und deren Kosten beantragt hatte, die Auskunftserteilung. Gegenüber der Krankenkasse, die die KVB-Auskunft zusammen mit ihrer eigenen Auskunft an den Versicherten weiter zu leiten hatte, argumentierte die KVB folgendermaßen: Die Umsetzung der Auskunftsverpflichtung sei derzeit nicht möglich, da zum einen die Angaben aus Datenschutzgründen nicht patientenbezogen an die Krankenkassen weitergegeben werden dürfen und diese Informationen zum anderen bei den manuell, also nicht per EDV abrechnenden Ärzten bei der KVB nicht patientenbezogen erfasst werden.

Dieser Weigerung der KVB, dem Patienten den ihm datenschutzrechtlich eingeräumten Auskunftsanspruch zu erfüllen, bin ich entgegengetreten. Neben der Verletzung des informationellen Selbstbestimmungsrechts des auskunftsbegehrenden Versicherten lief die Auskunftsverweigerung durch die KVB auch dem Bestreben des Gesetzgebers zuwider, die Kosten der Inanspruchnahme ärztlicher Leistungen durch die Auskunftspflicht gegenüber Versicherten transparent zu machen.

Die Prüfung ergab, dass die Umsetzung der Auskunftspflicht der KVB deshalb erhebliche Probleme bereitete, weil sie bisher davon abgesehen hatte, das für die Datenermittlung notwendige EDV-Programm zu erstellen und die Auskunftsanträge deshalb in zeitaufwändiger manueller Arbeit zu erledigen waren. Dies war der Hintergrund der Auskunftsverweigerung und nicht wie von der KVB zusätzlich vorgebracht, dass die KV nach § 305 Abs. 1 S. 2 SGB V die Auskunft **„in einer Form, die eine Kenntnisnahme durch die Krankenkasse ausschließt“ über die Krankenkasse** zu erteilen hat und diese gesetzlichen Vorgaben nicht erfüllbar wären. Auf meine Intervention hin erhielt der Petent die beantragte Auskunft auf dem beschriebenen Wege, also über die Krankenkasse in einem von der KVB verschlossenen Umschlag, den die Krankenkasse nicht öffnen durfte.

Infolge meiner Aufforderung, durch geeignete Maßnahmen sicherzustellen, dass die KVB-Bezirksstellen künftig dem § 305 Abs. 1 S. 2 SGB V entsprechende Auskünfte geben, hat die KVB ihre Bezirksstellen angewiesen, künftig gesetzeskonform nach obigem Lösungsvorschlag zu verfahren.

4.4.4 Schutz der Sozialdaten des KVB-Personals

Zum Schutz des Sozialgeheimnisses der Beschäftigten eines Sozialleistungs- bzw. Sozialversicherungsträgers (sowie der Angehörigen dieser Beschäftigten) verlangt § 35 Abs. 1 S. 3 SGB I, dass Sozialdaten der Beschäftigten und ihrer Angehörigen den Personen, die bei der datenspeichernden SGB-Stelle Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden dürfen.

Die Umsetzung dieser Vorschrift bereitet bei einer Kassenärztlichen Vereinigung Schwierigkeiten: Anders nämlich als bei Mitarbeitern einer Krankenkasse, die es durch Auswahl ihrer Kassenmitgliedschaft verhindern können, dass ihren Vorgesetzten und ihren Kollegen die sie betreffenden Patientendaten bekannt werden, ist eine vergleichbare „Steuerungsmöglichkeit“ für KV-Bedienstete praktisch kaum zu erreichen. Der Vertragsarzt ist nämlich verpflichtet, mit der KV abzurechnen, deren Mitglied er ist (§ 77 Abs. 3 S. 1, 294 und 295 Abs. 1 SGB V). Der bei der KV beschäftigte Patient hat rechtlich keine Möglichkeit, den Vertragsarzt zur Abrechnung von dessen Leistungen (mit damit verbundenen sensiblen medizinischen Patientendaten) bei einer anderen als der für diesen Arzt zuständigen KV zu veranlassen.

Da es generell misslich ist, wenn Arbeitskollegen/-innen Kenntnis über Patientendaten der Belegschaft des Betriebes erlangen können, habe ich die KVB aufgefordert, die Patientendaten des KVB-Personals über die gesetzliche Verpflichtung nach § 35 Abs. 1 S. 3 SGB I hinaus auch gegenüber Personen zu schützen, die lediglich Kollegen/-innen sind und keine Personalentscheidungen treffen oder daran mitwirken können.

Meinerseits habe ich die KVB um Überprüfung des folgenden Lösungsansatzes gebeten:

Die KVB-Bezirksstellen werden von der KVB-Landesgeschäftsstelle in die Lage versetzt, bei der Übernahme eingehender Arztrechnungen in den EDV-Bestand der KVB systemtechnisch Namen und Krankenversicherten-Nummern von KVB-Mitarbeitern zu erkennen. Die EDV verschlüsselt daraufhin im KVB-Datenbestand sofort die identifizierenden Daten der KVB-Mitarbeiter aus der Krankenversichertenkarte (vgl. § 291 Abs. 2 Nr. 2 bis 5 SGB V).
Freilich muss sichergestellt werden, dass der Mitarbeitername dennoch auf dem Datensatz wieder lesbar ist, der der Krankenkasse zur Überprüfung der Leistungspflicht übermittelt wird (vgl. § 295 Abs. 2 SGB V i.V.m. dem hierzu abgeschlossenen Datenträgeraustausch-Vertrag).

Außerdem muss die KVB in berechtigten Fällen (vgl. insbesondere § 285 Abs. 2 SGB V) in der Lage sein, den verschlüsselten Patienten ausnahmsweise zu identifizieren. Hierfür könnte eine Zugriffsbeschränkung auf wenige Vertrauenspersonen in der KVB (vgl. allerdings wiederum § 35 Abs. 1 S. 3 SGB I) sowie eine spezielle Protokollierung solcher Zugriffe vorgesehen werden.

Die KVB hat sich für meinen Lösungsvorschlag bedankt und prüft derzeit, ob er realisiert werden kann bzw. welche sonstigen Maßnahmen in Betracht kommen. Ich hoffe, dass damit eine Verbesserung des Sozialdatenschutzes für KVB-Mitarbeiter/-innen erreicht wird.

4.5 Sozialhilfeverwaltung

4.5.1 Auskunftsersuchen von Sozialämtern über Unterhaltspflichtige und deren nicht getrennt lebende Ehegatten

Nach § 116 Abs. 1 Bundessozialhilfegesetz (BSHG) muss u.a. der gegenüber einem Sozialhilfeantragsteller bzw. –bezieher Unterhaltspflichtige dem Sozialhilfeträger über seine Einkommens- und Vermögensverhältnisse Auskunft geben, soweit die Durchführung des BSHG es erfordert. Kommt er dieser Auskunftsverpflichtung nicht nach, ist das Sozialamt berechtigt, die benötigte Auskunft bei den Finanzbehörden zu erheben. Die Finanzbehörden haben nach § 21 Abs. 4 SGB X „Auskunft über die ihnen bekannten Einkommens- oder Vermögensverhältnisse des Antragsstellers, Leistungsempfängers, Erstattungspflichtigen, Unterhaltsverpflichteten, Unterhaltsberechtigten oder der zum Haushalt rechnenden Familienmitglieder zu erteilen“, soweit es im Verfahren nach dem Sozialgesetzbuch, beispielsweise im BSHG-Feststellungs- und Leistungsverfahren, erforderlich ist.

Im Jahre 1996 hat der Gesetzgeber die **Auskunftspflicht** in § 116 Abs. 1 BSHG **auf die nicht getrennt lebenden Ehegatten** der o.g. Unterhaltspflichtigen **erweitert**. Die Erweiterung betrifft die Fälle, in denen diese **Ehegatten nicht selbst** gegenüber dem Sozialhilfeantragsteller bzw. -bezieher **unterhaltspflichtig** (und nicht schon deshalb dem Sozialamt auskunftspflichtig) sind wie bspw. gegenüber Schwiegereltern und Stiefkindern. Der Wortlaut von § 21 Abs. 4 SGB X wurde in diesem Zusammenhang nicht geändert.

Aufgrund einer Eingabe war hinsichtlich der letzten Alternative in § 21 Abs. 4 SGB X **(„..oder der zum Haushalt rechnenden Familienmitglieder...“)** zu klären,

- ob sich aus dieser Gesetzesformulierung in Verbindung mit der besagten Erweiterung der Auskunftspflicht nach § 116 Abs. 1 BSHG auf die nicht getrennt lebenden Ehegatten der o.g. Unterhaltspflichtigen auch eine **Auskunftsverpflichtung der Finanzbehörden hinsichtlich dieser Ehegatten** ergibt (soweit die Ehegatten nicht selbst zur erforderlichen Sachverhaltsaufklärung beitragen) oder

- ob sich die genannte Alternative ausschließlich auf die zum Haushalt rechnenden **Familienmitglieder des Leistungsantragstellers bzw. –beziehers**, also bspw. auf die mit dem Hilfe Suchenden in einer Haushaltsgemeinschaft i.S.d. § 16 BSHG lebenden Person anwenden lässt mit der Folge, dass die Finanzbehörden keine Auskünfte über die Einkommens- oder Vermögensverhältnisse der gegenüber einem Sozialleistungsantragsteller/-bezieher nicht selbst unterhaltspflichtigen Ehegatten von Unterhaltspflichtigen erteilen dürfen.

Da sich die Auslegung zugunsten einer weitergehenden Auskunftspflicht (erster Aufzählungspunkt) mit dem Wortlaut des § 21 Abs. 4 SGB X vereinbaren lässt, bestand und besteht keine Notwendigkeit, diese Vorschrift der erweiterten Auskunftspflicht in § 116 Abs. 1 BSHG anzupassen:
Ebenso wie § 116 Abs. 1 BSHG, der dem Sozialhilfeträger die Ermittlung vorhandenen Einkommens und Vermögens zur Berechnung und Durchsetzung auf ihn nach § 91 BSHG übergegangener Unterhaltsansprüche ermöglichen soll, dient auch § 21 Abs. 4 SGB X der Vermeidung unberechtigter Sozialleistungen. Soweit die nicht getrennt lebenden Ehegatten von Unterhaltspflichtigen ihrer Auskunftspflicht nach § 116 Abs. 1 BSHG gegenüber dem Sozialamt nicht selbst nachkommen, sehe ich keinen Grund, weshalb die Finanzbehörden dem Sozialhilfeträger nach § 21 Abs. 4 SGB X bei Erforderlichkeit keine Auskünfte über die ihnen bekannten Einkommens- oder Vermögensverhältnisse auch betreffend diesen Personenkreis erteilen dürften. Auch wenn Finanzbehörden nicht ohne weiteres beurteilen können, inwieweit von einem Sozialleistungsträger erbetene Auskünfte für dessen Verwaltungsverfahren tatsächlich erforderlich sind, haben sie ihre Übermittlungsbefugnis anhand der §§ 30 ff. AO 1977 aufgrund der Bedeutung des Steuergeheimnisses dennoch möglichst sorgfältig zu prüfen. Dies gilt auch wegen des bei Übermittlungsersuchen eines Sozialleistungsträgers anzuwendenden § 67 d Abs. 2 S. 2 SGB X, wonach dieser zwar die Verantwortung für die Richtigkeit seiner Angaben, nicht aber (wie nach Art. 18 Abs. 2 S. 2 BayDSG) die Verantwortung für die Zulässigkeit der Beantwortung seiner Anfrage durch das Finanzamt insgesamt trägt. Die Finanzbehörde darf sich deshalb nicht auf eine knappe Schlüssigkeitsprüfung i.S.d. Art. 18 Abs. 2 S. 3 BayDSG beschränken, wonach die übermittelnde Stelle nur überprüft, „ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt“. Die Erforderlichkeit der Auskunft für die Aufgabenerfüllung seitens des anfragenden Sozialleistungsträgers (als ein Bestandteil der Zulässigkeit der Datenübermittlung) muss daher im Auskunftsersuchen dargelegt werden; Details dazu braucht und darf der Sozialleis-

stungsträger aber nur angeben, soweit dies zur Begründung seines Ersuchens und damit zur Entscheidung der Finanzbehörde erforderlich ist.

Im Ergebnis darf die Finanzbehörde den Sozialämtern also gemäß § 21 Abs. 4 SGB X und nach Maßgabe des § 116 Abs. 1 BSHG Auskunft über Einkommens- und Vermögensverhältnisse ggf. auch der nicht getrennt lebenden Ehegatten von Unterhaltspflichtigen geben, wenn das um Auskunft ersuchende Sozialamt darlegt, dass diese Auskunft der Finanzbehörde zu seiner Aufgabenerfüllung nach dem BSHG erforderlich ist. Ich weise die Sozialämter deshalb auf ihre Verpflichtung hin, Auskünfte der Finanzbehörden nach § 21 Abs. 4 SGB X erst dann und nur dann einzuholen, wenn die Betroffenen ihrer Auskunftspflicht nach § 116 Abs. 1 BSHG nicht selbst oder nicht in ausreichendem Umfang nachgekommen sind oder wenn die Richtigkeit seitens dieser Personen erteilter Auskünfte fraglich ist.

4.5.2 Behandlungskarte für Sozialhilfeempfänger

In der gesetzlichen Krankenversicherung Versicherte, die ärztliche oder zahnärztliche Behandlung in Anspruch nehmen, haben dem Arzt (Zahnarzt) gemäß § 15 Abs. 2 SGB V vor Beginn der Behandlung ihre Krankenversichertenkarte (§ 291 SGB V) auszuhändigen. Gemäß § 291 Abs. 1 S. 3 SGB V darf die Krankenversichertenkarte nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern (insbesondere Ärzte, Krankenhäuser, Apotheken usw.) verwendet werden. § 291 Abs. 2 SGB V regelt, welche Angaben die Krankenversichertenkarte ausschließlich enthalten darf. Es handelt sich dabei ausschließlich um nicht-medizinische Verwaltungsdaten.

Nicht in der gesetzlichen Krankenversicherung versicherte Sozialhilfeempfänger in Bayern erhalten vom Sozialamt Berechtigungsscheine zur Inanspruchnahme ärztlicher Behandlung (vergleichbar dem früheren „Krankenschein“) jeweils für ein Quartal ausgestellt. Auf diesen Behandlungsscheinen werden Name, Anschrift und Geburtsdatum des Betroffenen, Abrechnungsstelle (KVB) und Kostenträger (Kommune - Sozialamt -) sowie die Gültigkeitsdauer angegeben. Da dies ein aufwändiges und gemessen am Einsatz der Krankenversichertenkarte in der gesetzlichen Krankenversicherung ein wenig zeitgemäßes Verfahren darstellt und weil die Krankenhilfeleistungen der Sozialhilfe ohnehin den Leistungen der gesetzlichen Krankenkassen entsprechen sollen, ist in einem Pilotprojekt der Spitzenverbände der Krankenkassen mit dem Sozialamt der Stadt Augsburg vorgesehen, eine „Krankenversichertenkarte für Sozialhilfeempfänger“ mit der Bezeichnung „Behandlungskarte“ zu erproben. Laut Verfahrensbeschreibung orientieren sich Aufbau und Gestaltung dieser Karte an der Versichertenkarte der gesetzlichen Krankenkassen, da andernfalls eine maschinelle Lesbarkeit in den Arztpraxen nicht gegeben ist. Die Ärzte, die einen Sozialhilfeempfänger behandeln, können ihre erbrachten Leistungen durch Verwendung dieser Karte wie bei vertragsärztlichen Behandlungen an krankenversicherten Patienten über ihre Praxis-EDV mit der Kassenärztlichen Vereinigung Bayerns (KVB) abrechnen. Die KVB erstattet dem Arzt die aufgewendeten Kosten. Danach stellt die KVB der jeweiligen Kommune die für den Hilfeempfänger an den Arzt geleisteten Beträge in Rechnung.

Die Stadt Augsburg hat mich um datenschutzrechtliche Stellungnahme zu diesem Pilotprojekt gebeten.

Ich habe der Stadt Augsburg empfohlen, die Karte statt als „Betreuungskarte“ als „Behandlungskarte“ zu bezeichnen, da der Begriff der „Betreuung“ ein Rechtsbegriff aus dem Bürgerlichen Gesetzbuch (§§ 1896 bis 1908 k BGB) ist, mit dessen Voraussetzungen die Betreuungskarte für Sozialhilfeempfänger absolut nichts zu tun hat. Darüber hinaus habe ich angeregt, statt der Bezeichnung „Sozialamt“ als Kostenträger ausschließlich die „Stadt Augsburg“ auf der Behandlungskarte zu speichern bzw. zu nennen. Viele Sozialhilfeempfänger empfinden es als belastend, ihre Sozialhilfeempfänger-Eigenschaft beim Arzt vorlegen zu müssen. Soweit keine sachlichen Gründe entgegenstehen, sollte diese Problematik durch Angabe lediglich der Kommune statt des Sozialamts entschärft werden. Derzeit wird noch geklärt, ob die Angabe „Sozialamt“ auf der Karte zum schnellen Erkennen der Kartenverträglichkeit mit der Arzt-EDV sowie wegen eventueller Probleme bei der Abrechnung zwischen der KVB und der Stadt Augsburg oder bei der Abgrenzung innerhalb der Kommune erfolgen muss oder ob sie entfallen kann.

Ich habe der Stadt Augsburg im Übrigen mitgeteilt, dass ich keine grundsätzlichen Bedenken gegen das vorgesehene Pilotprojekt habe, wenn bei der Projektausgestaltung und –durchführung folgende zwingende Voraussetzungen eingehalten werden:

- Die Karte darf analog § 291 Abs. 1 S. 3 SGB V nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden.

- Die technische Absicherung der Karte, insbesondere gegen unbefugtes Beschreiben oder Überschreiben, muss identisch mit dem Sicherheitsstandard der Krankenversichertenkarte sein.

- Weitere Angaben als diejenigen, die dem Inhalt der Krankenversichertenkarte nach § 291 Abs. 2 Nr. 1 bis 8 SGB V entsprechen, dürfen auf der Karte keinesfalls gespeichert werden, **insbesondere keine medizinischen Daten**.

Soweit erforderlich darf die Behandlungskarte also höchstens die mir in der Verfahrensbeschreibung abschließend genannten Angaben enthalten. Ich habe die Stadt Augsburg um nochmalige Überprüfung gebeten, ob nicht auf die darin vorgesehene, wenn auch mit Schlüsselnummern belegte Bezeichnung als Hilfeempfänger/Haushaltsvorstand oder als Familienmitglied (Haushaltsangehöriger) verzichtet werden kann. Weshalb eine entsprechende Kennzeichnung „aus Gründen der Zuordnung des Falles“ notwendig sein sollte, erscheint mir nicht hinreichend dargelegt, zumal ich dem Muster des bisher vom Sozialamt verwendeten Behandlungsscheins keine derartige Aufgliederung entnehmen kann.

Ergänzend ist zu diesem Pilotprojekt anzumerken, dass Sozialhilfeempfänger nach dem BSHG Anspruch auf eine angemessene und sozialtypische Hilfegewährung haben. Da auch Versicherte in der gesetzlichen Krankenversicherung nach § 15 Abs. 2 SGB V die Krankenversicherten-Chipkarte verwenden müssen, erachte ich einen Zwang zur Verwendung der Behandlungskarte, der für den Teilnehmerkreis am Pilotverfahren im Bereich des Sozialamts der Stadt Augsburg wohl besteht, für sozialtypisch und sozialadäquat und damit bedenkenfrei. Jedenfalls solange die Behandlungskarte für Sozialhilfeempfänger nicht flächendeckend im Bundesgebiet zum Einsatz kommt, sehe ich keinen Anlass, das Projekt wegen Fehlens einer dem § 291 SGB V entsprechenden Norm im BSHG abzulehnen, soweit und solange die o.g. Voraussetzungen (vgl. Aufzählungspunkte) eingehalten werden.

4.6 Jugendämter

4.6.1 Datenübermittlungen im Fall „Mehmet“

Im Berichtszeitraum habe ich das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit (Sozialministerium) und das Bayerische Staatsministerium des Innern (Innenministerium) wegen der Weitergabe eines Briefes des Stadtjugendamts betreffend den türkischen Jugendlichen „Mehmet“ an das Ausländeramt der Landeshauptstadt München beanstandet.

Das Sozialministerium hatte unter Hinweis auf eine vorgesehene Besprechung „mit der Rechtsaufsichtsbehörde, dem StMI“ beim Stadtjugendamt München um einen Bericht insbesondere über die bisherigen Maßnahmen und Angebote der Jugendhilfe, über die Zusammenarbeit mit den Eltern und der Schule und über eventuelle weitere Hilfemöglichkeiten gebeten. Das Stadtjugendamt war wegen des Hinweises auf das Innenministerium davon ausgegangen, dass die Anfrage des Sozialministeriums im Auftrag des Innenministeriums als oberer Rechtsaufsichtsbehörde der LHSt. München im Rahmen der Kommunalaufsicht erfolgte. (Die Kommunalaufsicht im Innenministerium war allerdings in keiner Weise in das Verfahren eingeschaltet worden.) In diesem Schreiben berichtete das Stadtjugendamt München sehr detailliert, insbesondere über die Entwicklung der Person „Mehmets“, z. B. durch Informationen über schulische Fördermaßnahmen und Leistungen, über Verstöße gegen Rechtsvorschriften, über den Ablauf der Beteiligung des Allgemeinen Sozialdienstes der Landeshauptstadt München (ASD) usw.. Berichtet wurde dabei auch über die Beratung der Familie „Mehmets“ in einem Familienzentrum sowie über eine psychologische Untersuchung „Mehmets“ in einer Beratungsstelle einschließlich der dortigen Befunde und inklusive des Ergebnisses eines Intelligenztests. In der Besprechung mit dem Innenministerium gab das Sozialministerium das Schreiben des Stadtjugendamts vollinhaltlich an das Innenministerium als Oberster Ausländerbehörde weiter, das dieses Schreiben seinerseits wiederum in vollem Umfang der Ausländerbehörde im Kreisverwaltungsreferat der LHSt. München zukommen ließ.

Zur datenschutzrechtlichen Bewertung ist Folgendes zu sagen:

Dem **Sozialministerium steht bisher keine unmittelbare personenbezogene Aufsichts- und Kontrollbefugnis hinsichtlich einzelner Jugendhilfevorgänge** zu. Es ist nicht Rechtsaufsichtsbehörde; eine Fachaufsicht gibt es bei den Angelegenheiten des eigenen Wirkungskreises nicht, um die es sich nach Art. 3 BayKJHG i.V.m. den Vorschriften der Gemeindeordnung (GO) vorliegend handelt. Bei **rechtsaufsichtlichen Maßnahmen des Innenministeriums** als oberer Rechtsaufsichtsbehörde über die LHSt. München (Kommunalaufsicht) betreffend das Stadtjugendamt ist das Sozialministerium aufgrund der Verordnung über die Geschäftsverteilung der Bayerischen Staatsregierung zu beteiligen. In solchen Fällen kann dem Sozialministerium eine Art „ Gutachter- bzw. Sachverständigenfunktion“ für die Rechtsaufsicht zufallen, wozu es dann auch in eine Datenübermittlung an die Rechtsaufsichtsbehörde eingeschaltet werden dürfte. Die Kommunalaufsicht im Innenministerium hatte das Sozialministerium vorliegend aber nicht an der Ausübung einer Rechtsaufsicht betreffend das Stadtjugendamt beteiligt.

Eine „Quasi-Fachaufsicht“ und eine vom Tätigwerden der Rechtsaufsichtsbehörde unabhängige zusätzliche Rechtsaufsichtsfunktion des Sozialministeriums mit entsprechender Datenerhebungsbefugnis – etwa zur fachlichen Unterstützung des Innenministeriums als Oberster Ausländerbehörde – ist der Gesetzeslage nicht zu entnehmen. Auch für eine Einwilligung „Mehmets“ bzw. seiner Eltern in eine Datenerhebung bzw. -übermittlung zur Überprüfung der Tätigkeit des Stadtjugendamts durch das Sozialministerium lagen keinerlei Hinweise vor. Lediglich bei der Bearbeitung von Eingaben der Betroffenen in deren eigener Sache ist eine Datenerhebung durch das Sozialministerium unmittelbar – also ohne Umweg über die Rechtsaufsichtsbehörde – bei einem Jugendamt (bzw. die Antwort der Jugendämter unmittelbar an das Sozialministerium) datenschutzrechtlich vertretbar. Nur in diesen Fällen kann ich davon ausgehen, dass die Betroffenen durch ihre Eingabe ihre Einwilligung in diesen Datenfluss erteilt haben.

Ich habe gegenüber dem Sozialministerium empfohlen, eine Klarstellung in der Verordnung über die Geschäftsverteilung der Bayerischen Staatsregierung anzuregen, was seine Zuständigkeit bei Eingaben und Petitionen betreffend Jugendämter anbelangt. Soweit Beschwerden über Jugendämter nämlich nicht von Betroffenen, sondern von außenstehenden Dritten eingereicht werden, kann weder von einer Einwilligung der Betroffenen noch von einer Transparenz dieser Datenflüsse ausgegangen werden.

Mangels Datenerhebungsbefugnis des Sozialministeriums im Fall „Mehmet“ war freilich auch keine entsprechende Datenübermittlungsbefugnis des Stadtjugendamts für die Berichterstattung gegenüber dem Sozialministerium gegeben. In Anbetracht der – wie sich gezeigt hat – komplizierten Zuständigkeitsfragen habe ich jedoch von einer Beanstandung der unzulässigen Datenübermittlung durch das Stadtjugendamt an das Sozialministerium abgesehen.

Das Sozialministerium ist meiner rechtlichen Beurteilung im Ergebnis beigetreten. Es hat mit dem Innenministerium Einigkeit darin erzielt, dass im Zuge des Dritten Verwaltungsreformgesetzes das Gesetz zur Ausführung des Sozialgesetzbuches ergänzt werden soll. Vorgesehen ist dabei die Kompetenzzuweisung, dass die fachliche Beurteilung bei der Rechtsaufsicht über die örtlichen Träger der Jugendhilfe (und über die Sozialhilfeträger) sowie die Zuständigkeit für die Überprüfung und Bearbeitung von Eingaben und Petitionen, die diese Träger betreffen, auf der Ebene der Staatsregierung dem Sozialministerium obliegt. Mit dieser Gesetzesänderung wird das Sozialministerium die zu dieser Aufgabenerfüllung erforderlichen Daten dann unmittelbar erheben dürfen, d.h. ohne das Innenministerium als Komunalaufsicht darum ersuchen zu müssen.

Beanstandet habe ich die Weitergabe des detaillierten Berichts des Stadtjugendamts durch das Sozialministerium an die Oberste Ausländerbehörde im Innenministerium. Des Weiteren wurde das Innenministerium beanstandet, weil es diesen Bericht seinerseits an die Ausländerbehörde der LHSt. München weitergegeben hatte:

Zur Klärung, ob durch diese Datenübermittlungen (letztlich an die Ausländerbehörde) im Ergebnis eine Beschwer „Mehmets“ und seiner Familie eingetreten ist, habe ich mich eingehend mit der Argumentation des Innenministeriums auseinander gesetzt, wonach die umfassende Berichterstattung bereits durch das Stadtjugendamt unmittelbar an die Ausländerbehörde hätte erfolgen müssen. Dies war nicht der Fall: Zwar hat ein Jugendamt die Ausländerbehörde nach den Vorschriften des Ausländergesetzes (AuslG) zu unterrichten, wenn es von bestimmten Ausweisungsgründen Kenntnis erlangt. Der Bericht des Stadtjugendamts, der eben nicht für die Ausländerbehörde gedacht war, ging jedoch weit über § 46 Nr. 2 AuslG hinaus, da er nicht nur Hinweise auf Verstöße gegen Rechtsvorschriften, sondern darüber hinaus z. B. Informationen über schulische Fördermaßnahmen und Leistungen, über die psychologische Untersuchung einschließlich Ergebnismitteilung und den Ablauf der ASD-Beteiligung enthielt. Des Weiteren hat

das Jugendamt zwar auf Anforderung der Ausländerbehörde eine Sozialprognose über Jugendliche abzugeben, bei denen ein Ausweisungsgrund vorliegt. Unabhängig davon, dass sich das Stadtjugendamt zum Zeitpunkt seiner umfangreichen Berichterstattung an das Sozialministerium laut eigener Aussage noch zu keiner Sozialprognose betreffend „Mehmet“ im Stande sah, enthielt diese Berichterstattung jedenfalls auch solche Angaben, die selbst als Begründung im Falle einer tatsächlich getroffenen Sozialprognose zu weitgehend wären. Im Zusammenhang mit der psychologischen Untersuchung und dem Intelligenztest wurden nämlich auch psychologische Befunde genannt, die gemäß § 77 Abs. 2 AuslG i.V.m. § 71 Abs. 2 S. 2 SGB X der Ausländerbehörde im vorliegenden Falle nicht zugänglich gemacht werden durften, weil ihr derartige ärztliche bzw. psychologische Informationen nur in bestimmten, hier nicht gegebenen Ausnahmefällen übermittelt werden dürfen.

Da also schon das Stadtjugendamt nicht befugt gewesen wäre, die entsprechenden Informationen über „Mehmet“ unmittelbar an die Ausländerbehörde zu übermitteln, durfte auch das Sozialministerium das Innenministerium in dessen Funktion als Oberster Ausländerbehörde nicht derart umfassend informieren. Dies ergibt sich außerdem schon daraus, dass das Sozialministerium die ausführliche Berichterstattung des Stadtjugendamts wie dargelegt auch selbst weder anfordern noch erhalten hätte dürfen.

Ebenso wenig durfte das Innenministerium die Informationen, die es bereits unzulässiger Weise vom Sozialministerium erhalten hatte, an die Ausländerbehörde weitergeben. Aus § 78 Abs. 1 S. 1 SGB X ergab sich für die Oberste Ausländerbehörde ein Verwertungsverbot des Jugendamtsschreibens. Wie sich gezeigt hat, hielt die Ausländerbehörde weitere Informationen für den Erlass der Ausweisungsverfügung ursprünglich auch gar nicht für erforderlich: Die Ausländerbehörde erhielt den an das Sozialministerium adressierten ausführlichen Bericht über „Mehmet“ nämlich erst nach Erlass der Ausweisungsverfügung.

4.7 Unfallversicherung

4.7.1 Rechnungskorrekturen auf Banküberweisungen

Wie ich aufgrund der Eingabe eines Arztes erfahren habe, begründeten zwei Unfallversicherungsträger Rechnungskorrekturen bzw. –kürzungen gegenüber abrechnenden Ärzten in der Form, dass die Begründungen dieser Rechnungskorrekturen in die Vordrucke für Banküberweisungen aufgenommen und dem betroffenen Arzt per Kontoauszug mitgeteilt wurden. Diese Rechnungskorrekturen wurden somit auch den mit der Überweisung befassten Bankangestellten bekannt. Außerdem wurde es den betroffenen Ärzten erheblich erschwert, ggf. nicht erforderliche Kenntnisnahmen von solchen Begründungen etwa seitens der Steuerberater und ggf. Steuerprüfer der Finanzverwaltung zu vermeiden.

Ich habe den Unfallversicherungsträgern mitgeteilt, dass die bisherigen Mitteilungen auf Kontoauszügen allenfalls dann weiterhin hätten praktiziert werden können, wenn gem. § 67 b Abs. 2 SGB X schriftliche Einwilligungen der betroffenen Ärzte vorliegen oder noch eingeholt worden wären. Eine anderweitige gesetzliche Übermittlungsbefugnis nach dem SGB besteht nicht. Insbesondere ist diese Form der Datenübermittlungen nicht erforderlich zur Aufgabenerfüllung der Unfallversicherung nach § 199 SGB VII. Die Begründungen für Rechnungskorrekturen bzw. –kürzungen lassen sich nämlich ohne Möglichkeit zur Kenntnisnahme durch Dritte unter Anwendung entsprechender EDV-Programme auch per Post mitteilen, wie dies andere Unfallversicherungsträger handhaben.

In ihren Stellungnahmen beriefen sich die beiden betroffenen Unfallversichungsträger auf den bei einem Einzelversand der Korrekturtexte per Post entstehenden finanziellen Mehraufwand. Das Einholen schriftlicher Einwilligungserklärungen wurde wegen der Vielzahl von Ärzten, die mit diesen Unfallversicherungsträgern zusammenarbeiten, als nicht verwaltungspraktikabel abgelehnt.

Auf ihre Nachfrage, ob die Korrektur- bzw. Kürzungsbegründungen auf den Überweisungsträgern als **Sozialdaten** zu bewerten seien und unter das Sozialgeheimnis fallen, habe ich den Unfallversicherungsträgern Folgendes dargelegt: Betroffener i.S.d. § 67 Abs. 1 S. 1 SGB X ist vor-

liegend mangels Nennung zwar nicht der untersuchte bzw. behandelte Versicherte, im Zusammenhang mit dieser Überweisung aber der **Arzt**, dessen Rechnung mit der jeweiligen Begründung berichtigt bzw. gekürzt wurde und der auf der Überweisung notwendigerweise namentlich angegeben wird. Nicht nur personenbezogene Daten der Versicherten, sondern auch Abrechnungsbeträge und –korrekturen sowie Begründungen hierzu, die einen für den Unfallversicherungsträger tätig gewordenen Arzt betreffen, sind i.S.d. § 67 Abs. 1 SGB X Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten natürlichen Person, hier des Arztes. Diese Angaben werden vom Unfallversicherungsträger im Hinblick auf seine Aufgaben nach dem SGB übermittelt, da die Abrechnung für den Unfallversicherungsträger erbrachter ärztlicher Leistungen für diesen Sozialversicherungsträger eine Aufgabenerfüllung nach dem SGB VII darstellt. Somit sind (auch) Daten der von Abrechnungen des Unfallversicherungsträgers betroffenen Ärzte gem. § 67 Abs. 1 SGB X Sozialdaten.

Die beiden Unfallversicherungsträger haben mich daraufhin um Überprüfung gebeten, ob nicht wenigstens ein Teil der von ihnen verwendeten Mitteilungen datenschutzrechtlich hinnehmbar sei und weiterhin auf Banküberweisungen erfolgen dürfe. Ohne Einwilligung der Betroffenen erachte ich lediglich die Übermittlung **neutraler** Angaben auf den Überweisungsträgern für datenschutzrechtlich hinnehmbar, d.h. die Begründungen dürfen kein Fehlverhalten des Arztes und keine Korrektur des Berichtshonorares nach unten erkennen lassen.

Die beiden Unfallversicherungsträger haben mir mittlerweile mitgeteilt, dass sie die Begründungen für die Rechnungskorrekturen nach Umstellung der EDV-Programme künftig doch ausschließlich per gesonderter Post an die Ärzte versenden werden und zwar jeweils am Ende eines Monats. Zur Vermeidung zwischenzeitlicher Irritationen bei den Buchhaltungen der abrechnenden Ärzte werden die Überweisungsträger bzw. Kontoauszüge den folgenden datenschutzrechtlich unbedenklichen allgemeinen Hinweis enthalten: „Eventuelle Abweichungen vom Rechnungsbetrag werden jeweils am Monatsende schriftlich begründet“.

4.7.2 Gutachterauswahl nach § 200 Abs. 2 SGB VII und § 4 Abs. 2 und 3 BKV

Gemäß § 1 Ziffer 2 SGB VII ist es Aufgabe der Unfallversicherung, nach Maßgabe der Vorschriften des SGB VII nach Eintritt von Arbeitsunfällen oder Berufskrankheiten die Gesundheit und Leistungsfähigkeit der Versicherten mit allen geeigneten Mitteln wieder herzustellen und sie oder ihre Hinterbliebenen durch Geldleistungen zu entschädigen. Im Feststellungs- und Anerkennungsverfahren ihrer Leistungsverpflichtung sollen die Unfallversicherungsträger gemäß § 200 Abs. 2 1. Hs. SGB VII dem Versicherten vor Erteilung eines Gutachtenauftrags mehrere Gutachter zur Auswahl benennen. Zur Feststellung von Berufskrankheiten sieht § 4 der Berufskrankheiten-Verordnung (BKV) die Mitwirkung der für den medizinischen Arbeitsschutz zuständigen Stellen, regelmäßig also der Gewerbeärzte bzw. des Gewerbeärztlichen Dienstes vor. Diese sind über die Einleitung eines Feststellungsverfahrens betreffend eine Berufskrankheit unverzüglich schriftlich zu unterrichten und am weiteren Feststellungsverfahren zu beteiligen (§ 4 Abs. 2 BKV). Darüber hinaus haben die Unfallversicherungsträger gemäß § 4 Abs. 3 BKV die für den medizinischen Arbeitsschutz zuständigen Stellen über die Ergebnisse ihrer Ermittlungen zu unterrichten. Der Gewerbearzt/der Gewerbeärztliche Dienst kann, soweit die Ermittlungsergebnisse aus Sicht der für den medizinischen Arbeitsschutz zuständigen Stelle nicht vollständig sind, dem Unfallversicherungsträger ergänzende Beweiserhebungen vorschlagen. Hierzu bestimmt § 4 Abs. 3 S. 2 2. Hs. BKV, dass die Unfallversicherungsträger diesen Vorschlägen zu folgen haben.

Die zuletzt genannte Regelung warf im Berichtszeitraum wiederholt die Frage auf, ob der Unfallversicherungsträger eventuell auch an einen konkreten Gutachter gebunden ist, den der Gewerbearzt/Gewerbeärztliche Dienst in seinem ergänzenden Beweiserhebungsvorschlag angibt.

Eine solche Bindung des Unfallversicherungsträgers besteht nicht. Statt dessen ist er gemäß § 200 Abs. 2 1. Hs. SGB VII regelmäßig verpflichtet, dem Versicherten auch in den Fällen des § 4 Abs. 3 S. 2 BKV mehrere Gutachter zur Auswahl zu benennen. Dies ergibt sich bereits daraus, dass § 200 Abs. 2 SGB VII als höherrangiges Recht von einer Verordnungsbestimmung nicht abgeändert oder eingeschränkt werden kann. Leider hat das Bundesministerium für Arbeit und Sozialordnung mit genau dieser Begründung die Anregung des Bundesbeauftragten für den

Datenschutz abgelehnt, § 4 Abs. 3 BKV zur Klarstellung um den Satz „§ 200 Abs. 2 SGB VII bleibt unberührt“ zu ergänzen.

Wie meine Erkundigungen im Zusammenhang mit zwei Eingaben zeigten, vertreten auch die Unfallkasse München und die Bau-Berufsgenossenschaft Bayern und Sachsen die Rechtsauffassung, dass sich die Bindungswirkung ergänzender Beweiserhebungsvorschläge durch Gewerbeärzte/den Gewerbeärztlichen Dienst nicht auch auf einen darin ggf. enthaltenen konkreten Gutachtervorschlag erstreckt.

4.7.3 Prüfung der Abteilung „Arbeitsmedizinischer Dienst“ bei der Bau-Berufsgenossenschaft Bayern und Sachsen

Im Rahmen meiner regelmäßigen Kontrolle öffentlicher Stellen nach Art. 30 BayDSG habe ich die Abteilung „Arbeitsmedizinischer Dienst“ (AMD) bei der Bau-Berufsgenossenschaft Bayern und Sachsen datenschutzrechtlich geprüft. Gemäß Art. 1 Abs. 1 des Staatsvertrags über die Bestimmung aufsichtsführender Länder nach Art. 87 Abs. 2 S. 2 des Grundgesetzes führt der Freistaat Bayern die Aufsicht über die Bau-BG Bayern und Sachsen, da diese BG ihren Sitz in Bayern hat. Die Zuständigkeit für die Datenschutzkontrolle folgt der Zuständigkeit für die Aufsichtsbehörde.

Organisatorische Trennung des AMD von der Bau-BG im Übrigen

Nach § 24 Abs. 1 SGB VII können Unfallversicherungsträger überbetriebliche Arbeitsmedizinische Dienste einrichten. Die Dienste sind organisatorisch, räumlich und personell von den übrigen Organisationseinheiten des Unfallversicherungsträgers zu trennen. Die im Rahmen der Abschottung klärungsbedürftigen Punkte wurden in der „Dienstanweisung für die Abteilung Arbeitsmedizinischer Dienst (AMD) zur Ergänzung der bestehenden Regelungen für den Datenschutz und zur Wahrung der ärztlichen Schweigepflicht“ durch die Bau-BG datenschutzgerecht geregelt. Meine Kontrolle hat auch ergeben, dass die Bau-BG dem Trennungsgebot in der Praxis ebenfalls gerecht wird.

In personeller Hinsicht führt die Leitende Ärztin des AMD die Dienstaufsicht über ihre Mitarbeiter. Sie ist bei Anwendung der medizinischen Fachkunde im Verhältnis zur BG weisungsfrei. Die Bau-BG erteilt dem AMD keine fachlichen Aufträge. In Berufskrankheiten-Verfahren der BG wird der AMD grundsätzlich nicht eingebunden; nur gelegentlich richtet die BG Anfragen über Vorbefunde an den AMD. Entsprechende Auskünfte sowie in geeigneten Fällen eine beratende Einbeziehung des AMD in Verfahren der BG erfolgen ausschließlich bei Einwilligung des Betroffenen. Über die Erforderlichkeit der Weiterleitung medizinischer Unterlagen und Auskünfte des AMD an die BG entscheiden ausschließlich die Leiterin des AMD und ihr Stellvertreter. Dabei wird darauf geachtet, dass Anfragen der BG dem AMD die Überprüfung ermöglichen, inwieweit Informationen seitens des AMD an die BG erforderlich sind.

Alle Schreibarbeiten für den AMD werden ausschließlich von AMD-Mitarbeitern ausgeführt.

Zugang zu Räumen, in denen Akten und sonstige Unterlagen des AMD mit personenbezogenen Daten oder Betriebs- bzw. Geschäftsgeheimnissen (auch mikroverfilmt) aufbewahrt werden, wird ausschließlich befugten Mitarbeitern des AMD gewährt. Der AMD ist in einem eigenen Gebäudekomplex auf dem Grundstück der BG untergebracht.

Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen über den AMD der Bau-BG

Die Leitende Ärztin der Abteilung AMD ist ausschließlich dem Hauptgeschäftsführer der Bau-BG Bayern und Sachsen und seinem Stellvertreter unterstellt. Soweit sie diesen Geschäftsführern Bericht zu erstatten hat, bedarf es hierzu in aller Regel keiner versichertenbezogenen Angaben. Vor allem besteht keinerlei regelmäßige versichertenbezogene Informations- und Berichtspflicht der AMD-Leitung gegenüber der Hauptgeschäftsführung.

Soweit sie im Einzelfall für eine Maßnahme zur Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen durch die Hauptgeschäftsführung erforderlich ist, ist die Weitergabe von Sozialdaten durch den AMD an die Direktion der Bau-BG nach § 67 c SGB X zulässig. In Anbetracht der Dienst- und Aufgabenstellung der Hauptgeschäftsführung für alle Einrichtungen des Unfallversicherungsträgers verstößt die Wahrnehmung der vorstehenden Aufgaben nicht gegen

das Trennungsgebot. Freilich hat die Hauptgeschäftsführung dabei die absolute Zweckbindung der Sozialdaten ausschließlich für Aufgaben betreffend den AMD zu beachten.

Datenerhebungen, -nutzungen und –verarbeitungen durch den AMD im Zuge der Anwendung des Arbeitssicherheitsgesetzes (ASiG)

Die Teilnahme von Arbeitnehmern an allgemeinen arbeitsmedizinischen Vorsorgeuntersuchungen durch den AMD nach § 3 Abs. 1 Nr. 2 ASiG ist freiwillig. Dementsprechend erfährt nur der Arbeitnehmer die Ergebnisse solcher Untersuchungen, nicht aber der Arbeitgeber, außer im Falle einer freiwilligen Einwilligung des Arbeitnehmers in begründeten Einzelfällen. Mitteilungen bzw. Rücksprachen mit behandelnden Ärzten des Arbeitnehmers erfolgen nur im Falle einer Schweigepflichtsentbindung der AMD-Ärzte und der behandelnden Ärzte durch den jeweiligen Arbeitnehmer.

Datenerhebungen, -nutzungen und –verarbeitungen nach der Unfallverhütungsvorschrift VBG 100 i.V.m. § 15 Abs. 1 Nr. 3 SGB VII

Die Teilnahme an so genannten speziellen Vorsorgeuntersuchungen (§ 2 VBG 100) stellt für die Versicherten – mit Ausnahme spezieller Strahlenschutzuntersuchungen – eine Obliegenheit dar, d.h. der Arbeitgeber darf Versicherte, bei denen die Voraussetzungen für Vorsorgeuntersuchungen nach der VBG 100 gegeben sind, gemäß § 3 Abs. 1 VBG 100 an diesem Arbeitsplatz oder mit dieser Tätigkeit nur (weiter) beschäftigen, wenn sie fristgerecht Vorsorgeuntersuchungen unterzogen worden sind.

Gemäß § 9 Abs. 2 VBG 100 hat der ermächtigte Arzt/Betriebsarzt auch dem Arbeitgeber eine Bescheinigung über das Ergebnis dieser Untersuchungen, bezogen auf die dieser speziellen Vorsorgeuntersuchung zugrundeliegende gefährdende Tätigkeit auszustellen und ihm ggf. schriftlich eine Überprüfung des Arbeitsplatzes zu empfehlen, wenn der Versicherte wegen der Arbeitsplatzverhältnisse gefährdet erscheint. Diese durch § 9 Abs. 2 VBG 100 vorgesehene Datenübermittlung an den Arbeitgeber ist nach Maßgabe des § 15 Abs. 1 S. 1 Nr. 3 i.V.m. Abs. 2 S. 1 Nr. 9 SGB VII zulässig. Weil danach die **Übermittlung von Diagnosedaten an den Unternehmer verboten** ist, sind die Ergebnismitteilungen an Arbeitgeber gemäß Durchführungsanweisung zu

§ 9 Abs. 2 VBG 100 auf die Feststellungen zu beschränken, ob gesundheitliche Bedenken gegen eine Beschäftigung an einem bestimmten Arbeitsplatz bestehen oder nicht sowie auf ergänzend hierzu ausgesprochene Bedingungen oder Empfehlungen zur Überprüfung des Arbeitsplatzes. Untersuchungsbefunde und Diagnosen unterliegen dagegen der ärztlichen Schweigepflicht und dürfen – ebenso wie Empfehlungen an den Versicherten hinsichtlich medizinischer Maßnahmen – nur dem Versicherten bekannt gegeben werden.

Die bei der datenschutzrechtlichen Kontrolle überprüften Arbeitgebermitteilungen bei Untersuchungen nach der VBG 100 – im Übrigen auch die Ergebnismitteilungen an die Arbeitgeber bei arbeitsmedizinischen Vorsorgeuntersuchungen nach der Bildschirm-Verordnung (dort mit Einwilligung des Arbeitnehmers) – entsprachen diesen Beschränkungen.

Im Ergebnis hat die datenschutzrechtliche Kontrolle der Abteilung AMD der Bau-BG Bayern und Sachsen ein positives Bild hinsichtlich der Einhaltung datenschutzrechtlicher Bestimmungen ergeben.

4.8 Rentenversicherung

4.8.1 Datenschutz bei Arbeitgeberprüfungen nach § 28 p Abs. 1 SGB IV

Auf Anfrage eines Steuerberaters habe ich mich im Berichtszeitraum dazu geäußert, inwieweit die Prüfer der Rentenversicherungsträger bei Arbeitgeberprüfungen nach § 28 p SGB IV Einsicht in Unterlagen und Dateien verlangen dürfen, die nicht speziell die Lohn- und Gehaltsabrechnung betreffen, sondern einen darüber hinausgehenden Einblick in die Vermögensverhältnisse und geschäftlichen Dispositionen des Arbeitgebers gewähren. Zu beantworten war außerdem, ob eine Prüfung über den Bereich der Lohn- und Gehaltsabrechnung hinaus zu ihrer Zulässigkeit im Einzelfall ggf. besonders begründet werden muss.

Ziel der nach § 28 p SGB IV vorgeschriebenen Arbeitgeberprüfungen durch die Träger der Rentenversicherung ist insbesondere die Vollständigkeit und Richtigkeit der Zahlungen von Gesamtsozialversicherungsbeiträgen für die Arbeitnehmer. § 6 Abs. 3 S. 1 der Beitragsüberwachungsverordnung (BÜVO) in der Fassung der Änderungsverordnung vom 30.05.1996 berechtigt die Prüfer deshalb, „beim Arbeitgeber über den Bereich der Lohn- und Gehaltsabrechnung, jedoch nicht über den Bereich des Rechnungswesens hinaus zu prüfen“.

Wie mir seitens der Rentenversicherung nachvollziehbar dargelegt wurde, kommt der Ausdehnung der Prüfung über Lohn- und Gehaltskonten hinaus deshalb grundlegende Bedeutung zu, weil sich bei Prüfungen immer wieder zeigt, dass manche Arbeitgeber Sachverhalte konstruierten, um die Versicherungspflicht zu umgehen. Zwar kann die Prüfung der Lohn- und Gehaltsabrechnung bei so genanntem Lohnsplitting noch ausreichen, um eine versicherungs- und beitragsrechtliche Würdigung der Sachverhalte vornehmen zu können; wenn aber Löhne verdeckt ausgezahlt oder Lohnzahlungen nicht über Lohn- und Gehaltskonten gebucht werden, ist eine abschließende Prüfung der Versichungs- und Beitragspflicht nur unter Einbeziehung des gesamten Rechnungswesens möglich. Ebenso erfolgt die Abwicklung der Geschäftsvorfälle mit eventuellen Scheinselbstständigen – als Dienst- oder Werksvertragsleistungen – naturgemäß immer außerhalb der Lohn- und Gehaltsabrechnung, aber innerhalb des Rechnungswesens.

Auch die nach § 5 Abs. 5 BÜVO vorgeschriebenen versicherungs- und beitragsrechtlichen Auswertungen der Arbeitgeber-Prüfberichte der Finanzbehörden durch die Prüfer der Rentenversicherungsträger haben gezeigt, dass Zuwendungen an Arbeitgeber oftmals nicht als Arbeitslohn erkannt oder behandelt werden. Darüber hinaus werden selbst pauschal versteuerte Löhne teilweise außerhalb der Lohn- und Gehaltsabrechnung verbucht.

Stets hat der Arbeitgeber aber ein Interesse daran, Lohnkosten bzw. sonstige Aufwendungen im Rechnungswesen buchungsmäßig zu erfassen, damit sich die Kosten als Betriebsausgaben gewinnmindernd auswirken und seine Steuerpflicht senken. Dabei erfolgen Buchungen nicht selten auch auf Aufwandskonten wie z. B. Unterhaltung und Instandsetzung, Bewirtungskosten, Geschenke, Rabatte, Reisenkosten usw.; auch auf die Bestandskonten, Kapitalkonten, Ertragskonten sowie Lieferanten- und Kundenkonten können Buchungen erfolgt sein. Gelegentlich zahlen Arbeitgeber durch erhöhte Preise verdeckten Lohn, nämlich bei Übernahme (Nutzung oder Erwerb) von Sachen und Rechten vom Arbeitnehmer. Die Buchung erfolgt in den entsprechenden Aufwandskonten, ggf. auch auf Bestandskonten.

Um verdeckte Entgelte ermitteln und mögliche Fehlbeurteilungen der Versicherungspflicht benennen zu können, reicht es wegen dieser Möglichkeiten nicht aus, die Arbeitgeberprüfung auf die Lohn- und Gehaltsabrechnung zu beschränken, vielmehr darf gemäß § 6 Abs. 3 BÜVO das gesamte Rechnungswesen des Arbeitgebers in die Prüfung einbezogen werden.
Mit Änderungsverordnung vom 30.05.1996 hat der Verordnungsgeber in § 6 Abs. 3 S. 1 BÜVO die vormaligen beiden letzten Halbsätze („soweit es Gründe für die Annahme gibt, dass sich für die Versichungs- oder Beitragspflicht und die Beitragshöhe erhebliche Unterlagen auch außerhalb der Lohn- und Gehaltsabrechnung befinden“) gestrichen. Die Prüfung beim Arbeitgeber ist also seither im Bereich des Rechnungswesens außerhalb der Lohn- und Gehaltsabrechnung auch zulässig, **ohne dass dies besonders begründet werden muss**.

Im Rahmen der pflichtgemäßen Ausübung ihres Prüfungsermessens haben die Prüfer der Rentenversicherungsträger je nach Prüfungserfahrungen sowie nach der Sachlage des jeweiligen Einzelfalles zu entscheiden, inwieweit sie bei einer Arbeitgeberprüfung die Heranziehung von Unterlagen des Rechnungswesens als erforderlich ansehen.

Der vorstehend dargelegte Prüfungsumfang gilt gemäß § 7 Abs. 1 BÜVO entsprechend, wenn die Arbeitgeber-Prüfung statt bei diesem beim Steuerberater erfolgt, der im Auftrag des Arbeitgebers Löhne und Gehälter abrechnet. Aufgrund der bereichsspezifischen Prüfungsregelungen der §§ 28 p SGB IV, 6 und 7 BÜVO verstößt ein Steuerberater nicht gegen seine Verschwiegenheitspflicht nach § 57 StBerG, wenn er bei der Arbeitgeber-Prüfung über Unterlagen betreffend die Lohn- und Gehaltsabrechnung hinaus auch die von § 6 Abs. 3 BÜVO umfassten Unterlagen über den Bereich des Rechnungswesens im Übrigen vorlegt.

5 Polizei

5.1 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren:

- **Allgemeine Kontrolle von Speicherungen in Dateien und Karteien**, z. B im Kriminalaktennachweis (KAN), der Arbeitsdatei Rauschgift (ADR-neu), der Anhaltemeldung (AHM), der Datei Rauschgiftszene München, der Analysedatei bei sexuell motivierten Gewaltdelikten (ViCLAS), der Datei „Gewalttäter/Sport“, Staatsschutzdateien sowie von Dateien zur Gefahrenabwehr und Strafverfolgung (sog. GAST-Dateien)

- **Überprüfung von Errichtungsanordnungen für polizeiliche Dateien** (z. B Fahndungsdatei, Datei „Vorgetäuschte Verkehrsunfälle“, verschiedene Lagedateien sowie zahlreiche sog. GAST-Dateien)

- **Mitwirkung an der Überprüfung von Errichtungsanordnungen für Verbunddateien (bundesweite polizeiliche Dateien) und Dateien von EUROPOL** (z. B. DNA-Analysedatei, Automatisches Fingerabdruck-Identifizierungssystem (AFIS), Bundeskriminalaktennachweis, Europol-Analysedateien)

- wie in allen Berichtszeiträumen - teilweise aufgrund von Bürgereingaben - die **Kontrolle von Datenerhebungsmaßnahmen, Datenübermittlungen, Abfragen polizeilicher Informationssysteme sowie der Auskunftserteilung an Betroffene über Speicherungen in Dateien**

Ich habe an Gesetzen und Richtlinien sowie im Arbeitskreis Sicherheit mitgewirkt. Dazu kamen Vorträge an Aus- und Fortbildungseinrichtungen der Polizei

Im Berichtszeitraum habe ich wieder ein- und mehrtägige Prüfungen beim Bayerischen Landeskriminalamt, bei Polizeipräsidien, Polizei- und Kriminalpolizeidirektionen sowie deren nachgeordneten Dienststellen in ganz Bayern vorgenommen.

5.2 Ergebnis meiner Prüfungen und Bewertung von Grundsatzthemen

Bei meinen anlassunabhängigen Prüfungen von Polizeidienststellen und meinen Prüfungen aufgrund von Bürgereingaben und anderen Hinweisen habe ich durchweg eine datenschutzrechtliche Sensibilisierung bei der Polizei feststellen können. Bei den festgestellten datenschutzrechtlichen Verstößen handelte es sich in der überwiegenden Zahl soweit ersichtlich um Einzelfälle, die nachfolgender Darstellung entnommen werden können. Auch bei der Erörterung von Grundsatzthemen hat die Kooperations- und Kompromissbereitschaft der verantwortlichen Stellen zugenommen, wie z. B. meine ersten Beiträge zum Kriminalaktennachweis (KAN) zeigen. Leider gelingt es bisweilen nicht, mit dem Innenministerium datenschutzkonforme Problemlösungen in einem vertretbaren Zeitraum zu ergreifen. Nachfolgend werde ich auch die noch offenen Ergebnisse zu meinen Feststellungen im 18. Tätigkeitsbericht sowie die Problembereiche darstellen, bei welchen die Diskussion mit der Polizei und den verantwortlichen Ministerien noch nicht abgeschlossen ist.

5.3 Allgemeine Kontrolle von Speicherungen in Dateien und Karteien

5.3.1 Kriminalaktennachweis (KAN)

Der Kriminalaktennachweis (KAN) ist wohl das für die Bayerische Polizei bedeutendste und am meisten genutzte elektronische Informationssystem. Darin werden überwiegend Daten von Personen gespeichert, die keine Beschuldigten in einem Strafverfahren mehr sind. Diese Daten sind landesweit grundsätzlich für alle bayerischen Polizeivollzugsbeamten und z. T auch für Polizeiangestellte abrufbar. Wesentliche Voraussetzung für die Speicherung personenbezogener Daten im KAN ist, dass auch nach Abschluss des Strafverfahrens **ein Tatverdacht von ausreichender Substanz gegen die gespeicherte Person fortbesteht.** Dies ist regelmäßig der Fall bei der Verurteilung durch ein Gericht und sei es auch im Wege des Strafbefehlsverfahrens. Aber auch bei der Verfahrenseinstellung durch Gericht oder Staatsanwaltschaft und sogar bei einem gerichtlichen Freispruch kann der Tatverdacht gegen den Betroffenen fortbestehen, weil Anhaltspunkte für die Täterschaft sprechen, die aber für eine Anklageerhebung bzw. für eine Verurteilung nicht ausreichen. In den Fällen jedoch, in welchen der Tatverdacht entfallen ist, muss die Polizei die personenbezogenen Daten gem. Art. 38 Abs. 2 Satz 2 Polizeiaufgabengesetz (PAG) löschen.

In meinem 18. Tätigkeitsbericht habe ich darüber berichtet, dass die Anzahl der im KAN gespeicherten Personendatensätze im Vergleich zu den entsprechenden Speicherungen anderer deutscher Länder und dem Bund unverhältnismäßig hoch ist. Als mitursächlich für die hohe Zahl der Speicherungen waren nach meiner Auffassung von mir festgestellte systemimmanente Defizite und Mängel, die ich in meinem letzten Tätigkeitsbericht (vgl. Nr. 5.3.1 ff.) dargestellt habe.

Meine diesbezüglichen Verhandlungen mit den Staatsministerien des Innern und der Justiz sowie mit der Polizei sind neben anderen Feststellungen zum KAN im Folgenden dargestellt.

5.3.1.1 Speicherung nach Verfahrenseinstellung

In meinem 18. Tätigkeitsbericht habe ich u. a. bemängelt, dass die polizeiliche Prüfung der Speicherung von Verfahren, die von der Staatsanwaltschaft insbesondere gem. § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt wurden, unzureichend ist. Ich habe deshalb gefordert, dass die Polizei nach Mitteilung über die Einstellung des Verfahrens durch die Staatsanwaltschaft in jedem Fall nochmals selbst prüfen soll, ob ein Tatverdacht von ausreichender Substanz für die Speicherung noch vorhanden ist. Der Komplex konnte leider noch nicht abgeschlossen werden, Fortschritte wurden aber erzielt. Der Staatsminister des Innern hat mir dazu in Aussicht gestellt, die entsprechenden Vorschriften zu ergänzen und zu konkretisieren. Er hat folgende Formulierung vorgeschlagen:

„Vor Abgabe des Vorgangs an die Staatsanwaltschaft ist zu prüfen, ob eine Speicherung im KAN zur polizeilichen Aufgabenerfüllung erforderlich ist; dies gilt insbesondere bei Privatklage- und Fahrlässigkeitsdelikten. Dies gilt auch bei Rücklauf des Vorgangs von der Staatsanwaltschaft, sofern für die sachbearbeitende Polizeidienststelle erkennbar ist, dass die Staatsanwaltschaft eigene Ermittlungen vorgenommen hat, bei denen ggf. entlastende Erkenntnisse gewonnen wurden."

Dadurch solle erreicht werden, dass die Polizei **anhand ihrer Ermittlungsergebnisse** das Vorliegen eines substantiierten Tatverdachts (Anfangsverdacht) prüft. Nach Eingang der Einstellungsverfügung solle von der Polizei eine nochmalige Prüfung der Speicherung unter Berücksichtigung der Ermittlungstätigkeit der Staatsanwaltschaft vorgenommen werden in den Fällen, in denen diese eigene Ermittlungen ohne Beteiligung der Polizei vorgenommen hat, die über routinemäßige Registerabfragen hinausgehen. Allerdings seien dafür zusätzliche Informationen der Staatsanwaltschaft an die Polizei erforderlich, so dass eine Abstimmung mit dem Staatsministerium der Justiz notwendig sei.

In dieser Verfahrensänderung würde ich eine deutliche Verbesserung der Speicherungsprüfung sehen, da die endgültige Entscheidung der Polizei über die Speicherung der personenbezogenen Daten im KAN nicht bereits bei der Aufnahme des Ermittlungsverfahrens und der Anlage des Kriminalaktes erfolgen soll, sondern erst nach Abschluss der polizeilichen Ermittlungen. Hier-

durch würde sichergestellt, dass entlastende Ermittlungsergebnisse der Polizei bis zur Abgabe des Vorgangs an die Staatsanwaltschaft berücksichtigt werden können. Ein solches Verfahren würde eine individuelle Einzelfallprüfung und die Beachtung des Verhältnismäßigkeitsprinzips bei der Festlegung der Speicherungsfristen ermöglichen und dadurch die Gefahr unberechtigter Speicherungen verringern.

Sofern die Staatsanwaltschaft jedoch nach Abschluss der polizeilichen Ermittlungen noch eigene Ermittlungen durchführt und diese zu weiteren, den Betroffenen entlastenden Erkenntnissen führen, können diese Erkenntnisse bisher, mangels Mitteilung an die Polizei, keinen Eingang in die polizeiliche Entscheidung über die Datenspeicherung finden.

Ich habe daher für alle Fälle nachträglicher staatsanwaltschaftlicher Ermittlungen, die den Betroffenen entlasten, eine Mitteilung der Einstellungsverfügung mit Gründen an die Polizei gefordert, um diese so in die Lage zu versetzen, ihre Speicherungsentscheidung zu überprüfen. Das Staatsministerium der Justiz hat hierzu lediglich in Aussicht gestellt, die Übermittlung weiterer Daten im Rahmen des geplanten Datenaustauschs zwischen Justiz und Polizei zu überprüfen. Da ich aber die Mitteilung entlastender Erkenntnisse dringend für erforderlich halte, habe ich das Staatsministerium des Innern erneut um Stellungnahme gebeten, auf welchem Wege eine Berücksichtigung nachträglicher staatsanwaltschaftlicher Erkenntnisse bei der polizeilichen Speicherungsentscheidung sichergestellt werden soll.

Ich habe das Staatsministerium des Innern auch gebeten festzulegen, dass in Fällen der Einstellung des Verfahrens u. a. nach §§ 153 ff. StPO, 45, 47 Jugendgerichtsgesetz (JGG) ebenfalls eine nachträgliche polizeiliche Prüfung der Speicherung stattfindet. Zwar wird der Tatverdacht in diesen Fällen in der Regel fortbestehen, so dass eine Verfahrensbeendigung nach diesen Vorschriften nicht notwendigerweise eine erneute polizeiliche Überprüfung des Fortbestehens eines Restverdachts erfordert. Andererseits erfolgt eine Verfahrenseinstellung z. B. wegen geringer Schuld und fehlendem öffentlichen Interesse an der Strafverfolgung auch aus Gründen, die zumindest eine Bewertung der Tat als Fall geringerer Bedeutung i.S.d. Art. 38 Abs. 2 Satz 4 PAG (vgl. Nr. 5.3.1.4) mit **verkürzter Speicherfrist** nahelegen. Dabei ergeben sich die für diese Art der Einstellung maßgebenden Umstände nicht selten erst im Laufe des staatsanwaltschaftlichen

oder gerichtlichen Verfahrens. Die Information über eine derartige Einstellung sollte der Polizei zumindest Anlass zur Prüfung geben, ob eine Verkürzung der Speicherfrist vorzunehmen ist.

Eine endgültige Stellungnahme des Staatsministeriums des Innern, ob und ggf. in welchem Umfang diese Forderung umgesetzt und wie die Berücksichtigung eigener Ermittlungen der Staatsanwaltschaft sichergestellt werden, steht noch aus.

Ist der Tatverdacht entfallen, haben sowohl die Polizei als auch der Betroffene ein Interesse daran, die Gründe der Verfahrenseinstellung nach § 170 Abs. 2 StPO zu erfahren. Die Polizei wird hierdurch in die Lage versetzt, ihre Speicherung auf der Grundlage der durch die Staatsanwaltschaft vorgenommenen Bewertung zu überprüfen und ihrer Löschungsverpflichtung nachzukommen. Dem Betroffenen wird es ermöglicht, sein grundsätzlich bestehendes Recht auf Auskunft, ggf. Berichtigung, Sperrung oder Löschung gegenüber der Polizei wahrzunehmen. Eine ausreichende Unterrichtung ist deshalb dringend erforderlich:

- Die **Unterrichtung des Beschuldigten** von einer Verfahrenseinstellung gem. § 170 Abs. 2 StPO ist in Satz 2 dieser Vorschrift geregelt. Danach ist der Beschuldigte hiervon zu informieren, wenn er als solcher vernommen wurde, Haftbefehl gegen ihn erlassen war, er um einen entsprechenden Bescheid gebeten hatte oder ein besonderes Interesse an der Bekanntgabe ersichtlich ist. Liegt keiner dieser Gründe vor, wird der Betroffene über die Durchführung eines staatsanwaltschaftlichen Ermittlungsverfahrens sowie dessen Einstellung nicht informiert. Der Betroffene, der von dem Verfahren und dementsprechend von einer möglichen Speicherung bei der Polizei nichts wissen kann, hat gerade in den Fällen, in denen das Verfahren wegen erwiesener Unschuld oder Wegfall des Tatverdachts eingestellt wurde, ein besonderes Interesse, hiervon zu erfahren, um seine Rechte im Hinblick auf eine mögliche polizeiliche Datenspeicherung geltend machen zu können.

  Ich habe dem Staatsministerium der Justiz gegenüber ausgeführt, dass das Interesse des Betroffenen an der Geltendmachung seiner Rechte gegenüber der Polizei im Hinblick auf sein Recht auf informationelle Selbstbestimmung verfassungskonform als ein besonderes Interesse im Sinne von § 170 Abs. 2 StPO anzusehen sei, weshalb in allen Fällen der Verfahrenseinstellung wegen erwiesener Unschuld oder Wegfall des Tatverdachts eine Mitteilung an

den Betroffenen zu erfolgen habe.

Das Staatsministerium der Justiz war hiergegen der Auffassung, dass die Benachrichtungspflicht in § 170 Abs. 2 StPO als Ausnahme vorgesehen sei und diese gesetzgeberische Entscheidung zugunsten des Rechtsfriedens zu akzeptieren sei.

Ich sehe demgegenüber nicht, dass bei den gesetzgeberischen Überlegungen die polizeiliche Speicherung und ihre Konsequenzen für den Betroffenen bedacht wurden. Im Übrigen handelt es sich bei den wegen Wegfall des Tatverdachts eingestellten Fällen nur um eine relativ geringe Anzahl. Ich halte deshalb meine Forderung aufrecht.
Weiter hatte ich gegenüber dem Staatsministerium der Justiz angeregt, bei Einstellungsmitteilung gem. § 170 Abs. 2 StPO an den Beschuldigten diesen formblattmäßig darauf hinzuweisen, dass trotz Einstellung des staatsanwaltschaftlichen Ermittlungsverfahrens eine fortdauernde polizeiliche Datenspeicherung möglich ist. Das Staatsministerium der Justiz hat eine derartige Mitteilung abgelehnt, da sie im Hinblick auf weitere Datenspeicherungen bei anderen Stellen missverständlich wäre. Ich halte diese Ablehnungsbegründung nicht für durchschlagend.

- Für die **Unterrichtung der Polizei** von einer Verfahrenseinstellung gem. § 170 Abs. 2 StPO durch die Staatsanwaltschaft besteht bisher die Regelung, dass in den Fällen, in denen eine Mitteilung an den Beschuldigten zu erfolgen hat und der Wegfall des Tatverdachts durch die Staatsanwaltschaft festgestellt wurde, eine Einstellungsmitteilung **samt Begründung** an die Polizei zu erfolgen hat. Entsprechend einer Vereinbarung zwischen den Staatsministerien der Justiz und des Innern fordert die Polizei für diese Fälle formblattmäßig eine begründete Einstellungsmitteilung an. Eine Mitteilung der Gründe unterbleibt daher bisher schon in all jenen Fällen, in denen der Beschuldigte nicht vernommen wurde, kein Haftbefehl gegen ihn erlassen war, er nicht um einen Bescheid gebeten hatte und kein besonderes Interesse an der Bekanntgabe ersichtlich ist, und zwar auch dann, wenn der Tatverdacht entfallen ist.

  Auch in diesen Fällen besteht nicht nur ein Interesse der Polizei, sondern es ist notwendig, dass sie erfährt, dass die Staatsanwaltschaft vom Wegfall des Tatverdachts gegen den Betroffenen ausgegangen ist, da sie nach Art. 38 Abs. 2 Satz 2 PAG verpflichtet ist, die Speiche-

rung bei Wegfall des Tatverdachts zu löschen. Ebenso besteht ein dringendes Interesse des Betroffenen. Ich habe gegenüber dem Staatsministerium der Justiz sowie dem Staatsministerium des Innern hierauf hingewiesen und eine Mitteilung der Einstellungsgründe an die Polizei auch in solchen Fällen gefordert, in denen keine Beschuldigtenvernehmung durchgeführt wurde. Ohne diese Mitteilung erfährt die Polizei vom Wegfall des Tatverdachts nichts und wird deshalb vielfach ihrer Verpflichtung zur Löschung der Daten des Betroffenen im KAN nicht nachkommen. Ich habe darin einen unhaltbaren Zustand gesehen.

Das Staatsministerium der Justiz hat auf meine Intervention mit dem Staatsministerium des Innern vereinbart, dass die Polizei in allen Fälle der Verfahrenseinstellung wegen Wegfalls des Tatverdachts eine begründete Mitteilung von der Staatsanwaltschaft anfordert und erhält, unabhängig davon, ob eine Benachrichtigung auch des Betroffenen vorzunehmen ist.

5.3.1.2 Automatische Fristenverlängerung

In meinem 18. Tätigkeitsbericht hatte ich die Praxis der automatischen Fristenverlängerung polizeilicher Speicherungen dargestellt (vgl. Nr. 5.3.1.3). Ich hatte auch darauf hingewiesen, dass diese Praxis im Polizeiaufgabengesetz keine hinreichend klare gesetzliche Grundlage findet. Entsprechend hat auch der Bayerische Verwaltungsgerichtshof in seinem Urteil vom 04.06.1996 (BayVBl 1998, 115) die Rechtslage beurteilt. Mit der Änderung des Charakters der Speicherungsfristen (Regel- statt Höchstfristen) hat der Gesetzgeber auf Initiative der Staatsregierung ausdrücklich auch die automatische Fristverlängerung bei Hinzukommen neuer Speicherungen mit längerer Speicherungsfrist beschlossen.

Anlässlich meiner datenschutzrechtlichen Prüfung einer Polizeidienststelle habe ich automatische Fristenverlängerungen festgestellt, die sich weder auf die frühere noch auf die gegenwärtige Gesetzeslage stützen ließen.

Nach bundeseinheitlichen Vorschriften können unter bestimmten Voraussetzungen Personen in polizeilichen Informationssystemen zur Fahndung ausgeschrieben werden (z. B. wenn ein Haftbefehl gegen die Person vorliegt). Die Fahndungsausschreibungen sind Bestandteil des Informationssystems der Bayerischen Polizei (IBP) und ggf. des bundesweiten Informationssystems der

Polizei (INPOL). Diese Löschung einer Fahndungsausschreibung hatte eine automatische Fristenverlängerung für alle weiteren zur Person gespeicherten Unterlagen im KAN zur Folge. Im Einzelfall kann das eine Fristverlängerung bis zu zehn Jahren bedeuten.

Zwar beginnt die Speicherungsfrist nach Art. 38 Abs. 2 Satz 5 PAG nicht vor Entlassung des Betroffenen aus einer Justizvollzugsanstalt oder der Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Diese Regelung lässt sich aber nicht - wie vom BLKA angenommen - entsprechend auf den Zeitpunkt der Löschung der Fahndungsausschreibung übertragen. Das BLKA hat das akzeptiert und den Fehler bereinigt. Nunmehr wird nach Ablauf der Frist die Fahndungsausschreibung wie bisher gelöscht, die Löschung beeinflusst nicht mehr die Speicherungsdauer weiterer im KAN gespeicherter Unterlagen.

5.3.1.3 Manuelle Fristenverlängerung

Nach Art. 38 Abs. 3 PAG können abweichend von den Regelspeicherungsfristen (zehn Jahre bei Erwachsenen, fünf Jahre bei Jugendlichen und zwei Jahre bei Kindern) längere Fristen festgelegt werden, wenn die Voraussetzungen für eine polizeiliche Beobachtung nach Art. 36 PAG vorliegen. Dies ist der Fall, wenn die Gesamtwürdigung der Person **und** ihrer bisher begangenen Straftaten erwarten lassen, dass sie auch künftig Straftaten von erheblicher Bedeutung (vgl. Art. 30 Abs. 5 PAG) begehen wird oder Tatsachen die Annahme rechtfertigen, dass die Person Straftaten von erheblicher Bedeutung begehen wird. Eine Verlängerung der Speicherungsfrist um bis zu drei Jahren kommt unter den gleichen Voraussetzungen in Betracht.

Eine solche manuelle Fristenverlängerung habe ich bisher bei der Polizei mit einer Ausnahme nicht feststellen können. In diesem Fall wurde eine Speicherung unmittelbar vor Erreichen des Löschungs- bzw. Überprüfungszeitpunkts vom polizeilichen Sachbearbeiter um drei Jahre verlängert. Als Begründung war auf der Kriminalakte vermerkt: „Verlängert wegen Schwere der Tat“. Auf Nachfrage teilte mir die Polizei mit, dass bei dem Betroffenen Tatsachen die Annahme rechtfertigen würden, dass er Straftaten von erheblicher Bedeutung begehen werde. Der Betroffene sei wegen eines Verbrechens nach dem Betäubungsmittelgesetz (Haschisch-Schmuggel) zu einer Freiheitsstrafe verurteilt worden. Polizeiliche Erfahrungen zeigten, dass Personen, die

Rauschgifte in nicht geringen Mengen schmuggeln, diese nicht selbst konsumieren, sondern gewinnbringend verkaufen. Dabei werde das Entdeckungsrisiko mit der Folge einer Freiheitsentziehung von nicht unter einem Jahr in Kauf genommen. Aus polizeilicher Sicht müsse daher von entsprechenden weiteren Straftaten des Betroffenen ausgegangen werden. Somit sei aus polizeilicher Sicht eine Verlängerung der Aussonderungsprüffrist um weitere drei Jahre erforderlich.

Abgesehen von der unzureichenden Dokumentation der für die Verlängerung maßgeblichen Gründe konnte ich mich dieser polizeilichen Beurteilung nicht anschließen. Für „die Gesamtwürdigung der Person und ihrer bisher begangenen Straftaten“ lagen der Polizei außer der erst- und einmaligen Erkenntnis über den Betroffenen keine **Prognosekriterien** dafür vor, dass er als gefährlicher Intensivtäter anzusehen war. Die erstmalige Erkenntnis reicht für eine entsprechende negative Gesamtwürdigung nicht aus. Die Annahme der weiteren Begehung von Rauschgiftverbrechen lässt sich auch nicht auf Vermutungen und die kriminalpolizeiliche Erfahrung stützen. Notwendig sind Tatsachen, die eine solche Annahme rechtfertigen. Dies gilt umso mehr, da der Betroffene über zehn Jahre strafrechtlich nicht mehr in Erscheinung getreten war.
Die Voraussetzungen für die Verlängerung der Speicherungsfrist lagen daher nicht vor. Die Polizei hat sich meiner Auffassung angeschlossen, die Verlängerung der Aussonderungsprüffrist aufgehoben und die Speicherung gelöscht.

5.3.1.4 Speicherung von Fällen geringerer Bedeutung

Aufgrund einer vom Landtag beschlossenen Änderung des Art. 38 Abs. 2 PAG sind die dort genannten Speicherungsprüffristen (Erwachsene zehn Jahre, Jugendliche fünf Jahre, Kinder zwei Jahre) nunmehr Regelfristen. Allerdings ist in Art. 38 Abs. 2 PAG auch vorgesehen, dass in Fällen von geringerer Bedeutung kürzere Fristen festzusetzen sind. In den Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien) waren der Polizei Regelbeispiele für Fälle geringerer Bedeutung vorgegeben. Bei den Regelbeispielen handelte es sich um einige wenige Fahrlässigkeits-, Antrags- und Privatklagedelikte sowie weitere weniger bedeutende polizeiliche Sachverhalte ohne strafrechtlichen Bezug. Damit sollte aber nicht ausgeschlossen sein, dass in weiteren Fällen von vergleichbarem Gewicht eine geringere Bedeutung angenommen werden konnte. Durch Zufall habe ich erfahren (vgl. Nr. 5.10), dass darüber hinaus zum gleichen Regelungsbereich eine schriftliche Anordnung an die Präsidien der Polizei be-

stand, wonach es der Polizei untersagt war, über die in den PpS-Richtlinien genannten Regelbeispiele hinaus Fälle geringerer Bedeutung anzunehmen. Nachdem ich das aufgegriffen hatte, hat die Staatsregierung angekündigt, dass künftig auch außerhalb der Regelbeispiele im Einzelfall die Annahme eines Falles von geringerer Bedeutung möglich sei, so dass auf der Grundlage einer Entscheidung des Sachbearbeiters eine Verkürzung der Speicherfristen möglich sein werde.

Das Staatsministerium des Innern hat mir mitgeteilt, dass diese Änderung bei der Überarbeitung der PpS-Richtlinien berücksichtigt und die Polizei über die Änderung informiert werde. Im Hinblick auf diese Klarstellungen, durch die wesentliche Kritikpunkte meinerseits ausgeräumt werden, habe ich gegen oben genannte Gesetzesänderung keine Einwendungen mehr erhoben. Die entsprechende Überarbeitung liegt mir noch nicht vor. Ich habe mich deshalb erneut an das Staatsministerium des Innern gewandt.

Die Änderung der diesbezüglichen Praxis und deren Festlegung in den Richtlinien ist dringend notwendig, weil die bisherige Regelung den Vorgaben des Polizeiaufgabengesetzes nicht entspricht. Dieses geht nicht davon aus, dass Fälle geringerer Bedeutung auf einige wenige Deliktsgruppen beschränkt sind, sondern setzt eine individuelle Einzelfallprüfung der Tat und ihrer Umstände auch bei Delikten voraus, die vom Innenministerium bisher von einer solchen Prüfung generell ausgeschlossen waren. So ist nicht einsehbar, warum z. B. eine sog. Schwarzfahrt nicht als Fall geringerer Bedeutung in Betracht kommen sollte. Es ist notwendig, dass der polizeiliche Sachbearbeiter nach einer entsprechenden Änderung von dem ihm damit eröffneten Beurteilungs- und Entscheidungsspielraum sachgerecht Gebrauch macht, damit die Fristen unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit festgelegt werden.

Im Berichtszeitraum habe ich die Speicherung von Ordnungswidrigkeiten - die nach den PpS-Richtlinien regelmäßig Fälle geringerer Bedeutung sind - im KAN geprüft. Dabei habe ich festgestellt, das bei einer Polizeidirektion in sieben Fällen je eine Ordnungswidrigkeit zu den betroffenen Personen im KAN gespeichert war. Die Speicherung im KAN war unzulässig, weil wie ich in meinem 18. Tätigkeitsbericht (vgl. Nr. 5.3.1.5) dargestellt hatte, Fälle geringerer Bedeutung als alleinige Unterlage zur Person im KAN nicht nachgewiesen werden dürfen, sondern lediglich in den regionalen Vorgangsverwaltungsdateien. Ich habe die Polizeidirektion aufgefordert, die sieben Speicherungen im KAN zu löschen. Nach längerer Korrespondenz, die auf ein fehlerhaf-

ten Verständnis der Vorschriftenlage durch die Polizeidirektion zurückzuführen war, hat diese die Speicherungen gelöscht.

5.3.1.5 Vergabe von personengebundenen Hinweisen (PHW)

Die Speicherung von sog. personengebundenen Hinweisen im KAN (vgl. 18. Tätigkeitsbericht, Nr. 5.3.1.4), welche die Speicherung von polizeilichen Unterlagen ergänzen, habe ich wiederum bei verschiedenen Polizeidienststellen geprüft.

- Personengebundener Hinweis GEKR (geisteskrank)

  Meine Prüfungsfeststellungen zu der Speicherung des PHW GEKR hatte ich bereits in meinem 18. Tätigkeitsbericht (Nr. 5.3.1.4) dargelegt. Leider musste ich bei meinen erneuten Prüfungen wiederum feststellen, dass die Voraussetzung für die Speicherung dieses besonders sensiblen Datums - nämlich die dokumentierte ärztliche Feststellung von Geisteskrankheit - in mehreren Fällen nicht vorlag und die Speicherungen damit unzulässig waren. In einem Fall war lediglich dokumentiert, dass ein Verfahren gegen den Betroffenen gem. § 170 Abs. 2 StPO i.V.m. § 20 StGB eingestellt worden war. Eine Verfahrenseinstellung nach § 20 StGB (Schuldunfähigkeit) reicht für eine Speicherung des personengebundenen Hinweises GEKR nicht aus, da die Schuldunfähigkeit nicht auf einer Geisteskrankheit beruhen muss. Zu einer anderen Speicherung befand sich lediglich eine Kopie des Behindertenausweises des Betroffenen in der Kriminalakte. Auch hier fehlten die Voraussetzungen für die Speicherung des personengebundenen Hinweises. Eine weitere Speicherung basierte offenbar auf einem in der Kriminalakte befindlichen Vorgang über die Unterbringung in einem Bezirkskrankenhaus, ohne dass die vorgeschriebene ärztliche Feststellung oder behördliche Mitteilung über eine Geisteskrankheit vorlag. Die Polizeidienststellen wurden aufgefordert, den personengebundenen Hinweis zu löschen oder die erforderliche ärztliche Feststellung oder behördliche Mitteilung beizubringen. Die Antwort auf meinen Prüfbericht steht noch aus.

- Personengebundener Hinweis FREI (Freitodgefahr)

  Der personengebundene Hinweis FREI darf nach der Errichtungsanordnung vergeben wer-

den, wenn Anhaltspunkte dafür vorliegen, dass der Betroffene den Freitod suchen könnte, wobei für die Prognose ein zurückliegender Freitodversuch von Bedeutung sein kann. Der personengebundene Hinweise darf nur für die Dauer von zwei Jahren gespeichert werden. Bei meiner Überprüfung habe ich festgestellt, dass in drei Fällen FREI gespeichert war, obwohl die Speicherungsfrist von zwei Jahren bereits abgelaufen war. Ich habe die Polizei aufgefordert, die personengebundenen Hinweise zu löschen. Die Antwort auf meinen Prüfbericht steht noch aus.

5.3.1.6 Vergabe von KAN-Merkern

Bei der Speicherung im KAN werden zu jedem Sachverhalt von den polizeilichen Sachbearbeitern sog. KAN-Merker vergeben. Die Vergabe dieser Steuerungsmerker dient der Festlegung, ob die personenbezogenen Daten zum jeweiligen Sachverhalt ausschließlich im Landeskriminalaktennachweis oder darüber hinaus auch im Bundeskriminalaktennachweis gespeichert werden sollen. Zur Weitersteuerung in den Bundeskriminalaktennachweis stehen der bayerischen Polizei acht KAN-Merker zur Verfügung. Die Vergabe der KAN-Merker ist an bestimmte Voraussetzungen geknüpft, die im Einzelnen in der Errichtungsanordnung Personen- und Fall-Auskunftsdatei (PFAD) festgelegt sind. Ob die Voraussetzungen für die Vergabe des KAN-Merkers 2 (gewohnheits-/gewerbsmäßige Begehung von Straftaten) vorlagen, habe ich bei verschiedenen Polizeidienststellen geprüft.

Der KAN-Merker 2 kann vergeben werden, wenn ein Tatverdächtiger gewohnheits- oder gewerbsmäßig handelte. Nach der Definition in der Errichtungsanordnung PFAD handelt gewohnheitsmäßig, wer durch wiederholte Tatbegehung erkennen lässt, dass eine kriminelle Neigung vorliegt. Gewerbsmäßig handelt, wer sich aus wiederholten Straftaten eine nicht nur vorübergehende Einnahmequelle verschafft. Bei meiner datenschutzrechtlichen Prüfung einer Polizeidirektion habe ich festgestellt, dass bei zwei Personen, zu denen der KAN-Merker 2 vergeben war, jeweils nur eine Unterlage im KAN gespeichert war. Auch eine Überprüfung der den Speicherungen zugrundeliegenden Kriminalakten hat keine Anhaltspunkte für die Vergabe des KAN-Merkers 2 ergeben. Die Polizei hat den KAN-Merker daraufhin gelöscht. Damit ist die bundesweite Speicherung der Unterlagen entfallen.

5.3.1.7 Sperren von Daten

In meinem 18. Tätigkeitsbericht hatte ich dargestellt, dass die Löschung von polizeilichen Daten und die Vernichtung von Unterlagen zu unterbleiben hat, wenn Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt würden (vgl. Nr. 5.3.1.6). In diesen Fällen sind die Daten zu sperren und mit einem Sperrvermerk zu versehen. Schutzwürdige Interessen sind z. B. dann beeinträchtigt, wenn der Betroffene die Zulässigkeit der Verarbeitung seiner personenbezogenen Daten verwaltungsgerichtlich oder durch den Landesbeauftragten für den Datenschutz prüfen lassen will. Leider habe ich anlässlich einer Bürgereingabe feststellen müssen, dass eine Sperrung von Daten im Kriminalaktennachweis technisch nicht möglich ist. Das Staatsministerium des Innern hat mir aber auf Nachfrage mitgeteilt, dass das Landeskriminalamt beauftragt wurde, die Möglichkeit der Sperrung von KAN-Daten zu schaffen. Später erhielt ich die Mitteilung, dass eine Realisierung der technischen Sperrung im Kriminalaktennachweis u. a. wegen der EDV-technischen Verknüpfung des KAN mit dem bundesweiten Informationssystem INPOL in absehbarer Zeit nicht möglich sei. Zur Befriedigung der gesetzlichen Anforderungen (vgl. Art. 45 Abs. 3 Satz 2 PAG) habe es folgende Regelung angeordnet:

In Fällen, in denen einen Sperrung erforderlich ist, wird die entsprechende Speicherung im KAN gelöscht und die dazugehörigen Akten bzw. Unterlagen bei der jeweils aktenführenden Dienststelle beim dortigen behördlichen Datenschutzbeauftragten, getrennt vom übrigen Kriminalaktenbestand, aufbewahrt. Zu Zwecken der Dokumentation der zu löschenden Speicherung ist der Akte bzw. den Unterlagen ein Dateiausdruck beizugeben.
Dieses Verfahren halte ich für eine angemessene Ersatzlösung. Ich habe dem Staatsministerium des Innern deshalb mitgeteilt, dass ich hiergegen keine Einwände erhebe.

5.3.1.8 Speicherung von Alias-Personalien

Es haben sich wieder einige Bürger an mich gewandt, die bei polizeilichen Kontrollen gerade an der Grenze einer besonderen Überprüfung unterzogen wurden. Die Ursache lag darin, dass ihre personenbezogenen Daten missbräuchlich von Tatverdächtigen, insbesondere von polizeilich gesuchten Straftätern benutzt wurden. Falls diese missbräuchliche Benutzung fremder Personalien bekannt wird, werden auch diese Alias-Personalien Bestandteil der Fahndungsausschreibung des gesuchten Straftäters. In diesen Fällen bedarf es bei Kontrollen einer polizeilichen Abklärung der tatsächlichen Identität, was mit einer zeitlichen und nervlichen Belastung des nicht gesuchten Bürgers verbunden ist.

Ich halte die Fahndungsausschreibung der von einem Straftäter missbräuchlich benutzten Personalien für zulässig, wenn zu erwarten ist, dass die tatsächlich gesuchte Person künftig weiterhin unter dem Namen der nicht gesuchten Person auftritt. Allerdings hatte ich den für diese Fälle von der Polizei zur Vermeidung von Missverständnissen auf dem Fahndungsbildschirm gespeicherten Vermerk, dass die Personalien nicht mit denen der gesuchten Personen übereinstimmen für unzureichend gehalten (vgl. 18. Tätigkeitsbericht, Nr. 5.3.6). Das Innenministerium hatte daraufhin den Vermerk neu formuliert.

Aber auch diese datenschutzrechtliche Verbesserung kann bei einer erstmaligen Kontrolle der nicht gesuchten Person Verwechslungen und die damit verbundenen unangenehmen Folgen nicht ausschließen, da der Vermerk von der Polizei erst dann gespeichert werden kann, wenn dieser die missbräuchliche Benutzung von Personalien bekannt wird. Nach Mitteilung des Innenministeriums habe es alle bayerischen Polizeidienststellen angewiesen, in diesen Fällen den Vermerk zu speichern. Mir wurde allerdings im Rahmen einer Eingabe bekannt, dass die Speicherung von Amts wegen offenbar nicht erfolgt war. Der Betroffene war nach seinen Angaben den besonderen Kontrollen wiederholt ausgesetzt. Deshalb weise ich die Betroffenen, die sich an mich wenden, auf die Möglichkeit hin, bei der Polizei den Vermerk in der Personenfahndungsdatei speichern zu lassen. Dieser ist geeignet, Fehlbeurteilungen der Polizei bei Kontrollen zu vermeiden.

5.3.2 System zur Verknüpfung von Gewaltverbrechen (ViCLAS)

Wie ich in meinem 18. Tätigkeitsbericht bereits angekündigt hatte, habe ich die Speicherungen eines Polizeipräsidiums in dem Datenbanksystem ViCLAS geprüft. Schwerpunkt der Prüfung war die Speicherung von Personen wegen „verdächtigen Ansprechens von Kindern und Jugendlichen“. Die datenschutzrechtliche Problematik bei diesen Speicherungen liegt darin, dass auch Personen gespeichert werden sollen, bei denen noch kein die Einleitung eines strafrechtlichen Ermittlungsverfahrens ausreichender Tatverdacht i.S.d. § 152 der Strafprozessordnung (Anfangsverdacht) vorliegt oder deren Handlungen keinen Tatbestand eines Strafgesetzes erfüllen. Wie mir vom Staatsministerium des Innern dazu mitgeteilt wurde (vgl. Nr. 5.4.1, 18. Tätigkeitsbericht), liege ein verdächtiges Ansprechen im Sinne des Dateienzwecks dann vor, wenn das Verhalten einer Person ein sexuelles tatrelevantes Motiv erkennen lasse.

Meine Prüfung einer umfangreichen Auswahl dieser Speicherungen hat ergeben, dass diese Voraussetzungen erfüllt waren.

Das Datenbanksystem ViCLAS wurde zwischenzeitlich auch bei den Polizeien aller anderen Bundesländer eingeführt. Darüber hinaus ist nun auch eine Verbunddatei (vgl. Nr. 5.5) ViCLAS eingerichtet worden, in die die Länderpolizeien ihre Daten einstellen. Zugriff haben - entsprechend einer datenschutzrechtlichen Forderung nach einem eng begrenzten Kreis der Zugriffsberechtigten - nur die unmittelbar und ausschließlich mit der Fallanalyse betrauten sog. Fallanalytiker oder Profiler. Verdächtiges Ansprechen von Kindern und Jugendlichen soll nur dann zur Speicherung führen, wenn ein sexuelles Gewaltmotiv vermutet werden kann und nach Sachlage tatsächliche Anhaltspunkte für eine geplante schwerwiegende Straftat vorliegen.

Ich habe das Staatsministerium des Innern aufgefordert, die bayerische Errichtungsanordnung an die des Bundes anzugleichen. Insbesondere gilt das bezüglich der sog. Konkretisierung der Speicherungsvoraussetzungen für „Verdächtiges Ansprechen“, weil die bisherige bayerische Formulierung keine Aussage darüber trifft, in welcher Hinsicht der Betroffene bzw. sein Ansprechen verdächtig sein muss. Zum anderen gilt das auch für die Speicherung anderer Personen als Tatverdächtige (z. B. Opfer, Zeugen etc.), die grundsätzlich nur mit ihrer Einwilligung in ViCLAS

gespeichert werden sollten. Die Stellungnahme des Staatsministerium des Innern hierzu steht noch aus.

5.3.3 Datei „Gewalttäter/Sport“

Bereits im Vorfeld der Fußball-Europameisterschaft 2000 wurden die polizeilichen Maßnahmen zur Abwehr von Gewalttaten sog. **Hooligans** europaweit diskutiert. Eine dieser Maßnahmen ist die bundesweite Speicherung gewaltbereiter „Fußballfans“ in der Verbunddatei (vgl. Nr. 5.5) „Gewalttäter/Sport“. Die Datei soll dazu dienen, diesen Personenkreis rechtzeitig, insbesondere bei polizeilichen Vorkontrollen und anderen Begleitmaßnahmen im Rahmen von Fußballbundesligaspielen und ähnlichen Fußballereignissen zu erkennen, um geeignete und angemessene gefahrenabwehrende Maßnahmen (z. B. Platzverweis, Gewahrsam, Stadionverbot etc.) treffen zu können.

Aufgrund der Feststellungen eines anderen Landesbeauftragten für den Datenschutz bei der Prüfung von Speicherungen der Polizei seines Landes in der Datei „Gewalttäter/Sport“ habe ich diese Datei für den Bereich eines Polizeipräsidiums geprüft. Er hatte erfahren, dass Polizeien anderer Länder Speicherungen vornähmen, die mit den Vorgaben der Errichtungsanordnung (vgl. Nr. 5.4) nicht in Einklang stünden. So würden z. B. undifferenziert und ohne Prüfung des Einzelfalls alle Insassen einzelner Busse und Zugabteile gespeichert. Diesem Vorwurf bin ich bezüglich bayerischer Speicherungen nachgegangen.

Bei unseren Stichproben hat sich dieser Vorwurf nicht bestätigt. Bei den verhältnismäßig wenigen Speicherungen wurden die Vorgaben der Errichtungsanordnung eingehalten. Bei fast allen Gespeicherten war der Vorwurf berechtigt, dass es sich bei ihnen um gewaltbereite **Hooligans** handelt. Nur eine Person konnte nicht den Hooligans zugeordnet werden. Aber auch bei ihr war die Prognose bezüglich Gewaltbereitschaft aufgrund der polizeilichen Erkenntnisse zutreffend.

Anlass zur Kritik bestand allerdings hinsichtlich der Vergabe des personengebundenen Hinweises (PHW) „gewalttätig“. Wie beim KAN (vgl. 5.3.1.5) kann dieser Hinweis nach der Errichtungsanordnung auch im Rahmen der Datei „Gewalttäter/Sport“ vergeben werden. Die konkreten Speicherungsvoraussetzungen sind – mangels anderweitiger Vorgaben – den allgemeinen Rege-

lungen zur Speicherung des PHW im KAN zu entnehmen. Nach meinen Feststellungen war das Vorliegen der dort genannten Voraussetzungen „...dass der Betroffene bei einer Straftat erhebliche Gewalt gegen Personen oder Sachen eingesetzt hat“... bei einigen Speicherungen nicht erkennbar, weil die Gewalt von den Personen noch nicht eingesetzt worden war. Das Polizeipräsidium hat sich meiner Auffassung angeschlossen und die beanstandeten PHW gelöscht.

5.3.4 Anhaltemitteilung-Kfz-Fahndung (AHM)

Diese Datei dient der Unterstützung polizeilicher Fahndungsmaßnahmen bei der Bekämpfung der internationalen Kfz-Verschiebung. Speicherungen in dieser Datei habe ich bei einer Polizeidirektion an einer EU-Binnengrenze geprüft. Die Speicherungen in der Datei erfolgt - seit Wegfall der Grenzkontrolle - in der Regel anlässlich von verdachts- und ereignisunabhängigen Kontrollen (vgl. Nr. 5.6.1).

Bemängelt habe ich bei meiner Prüfung die unzureichende Dokumentation der Gründe für die Speicherung in der Datei. Ohne ausreichende Dokumentation ist eine nachträgliche Überprüfung der Zulässigkeit der Speicherung nicht oder nur bedingt möglich. Nachdem für die Speicherungen kein Aktenrückhalt angelegt wird, kann die Dokumentation der Speicherungsgründe nur in der Datei selbst oder auf dem von der Polizei verwendeten Erfassungsformblatt erfolgen. Die betroffene Polizeidirektion hat meine Forderung nach **ausreichender Dokumentation** dadurch umgesetzt, dass sie neben dem Freitextfeld des Formblatts nunmehr vier standardisierte Erfassungsgründe zur Auswahl anbietet. Diese wurden nach Mitteilung der Polizei aufgrund polizeilicher Erfahrungswerte im Kriminalitätsbereich „Kfz-Verschiebung“ ausgewählt. Daneben kann die Speicherung aber auch aus „sonstigen Gründen“ erfolgen. Die vier standardisierten Erfassungsgründe sind eng gefasst, was einerseits die Nachvollziehbarkeit der Speicherung verbessert, andererseits aber die Auswahl reduziert. Weil ich davon ausgehe, dass zahlreiche Speicherungen auch aus „sonstigen Gründen“ durchgeführt werden, habe ich gefordert, dass eine Erfassung aus „sonstigen Gründen“ freitextlich mit den **konkreten Gründen des Einzelfalls** ergänzt wird.

Im Rahmen meiner Prüfung von AHM-Speicherungen bei der Polizeidirektion habe ich auch festgestellt, dass diese personenbezogene Daten auch an Polizeidienststellen eines Staates übermittelt, der nicht EU-Mitglied ist. Danach wird anlässlich von polizeilichen Kontrollen in diesem

Staat auf Ersuchen der ausländischen Polizeidienststelle von der bayerischen Polizei u.a. mitgeteilt, ob der Betroffene in polizeilichen Dateien gespeichert ist.

Eine solche Datenübermittlung kann sich - soweit die Polizei aufgrund über- oder zwischenstaatlicher Vereinbarungen über Datenübermittlung zwischen Polizeidienststellen nicht dazu verpflichtet ist - nur auf Art. 40 Abs. 5 Nr. 2 PAG stützen. Danach kann die Polizei personenbezogene Daten auf Ersuchen an Behörden und sonstige Stellen außerhalb des Geltungsbereichs des Grundgesetzes übermitteln, soweit dies **zur Abwehr einer erheblichen Gefahr** durch den Empfänger erforderlich ist. Die von mir festgestellten Datenübermittlungen wurden nach Mitteilung der Polizei zur Bekämpfung der Kfz-Verschiebung durchgeführt. Erhebliche Gefahr ist eine Gefahr für ein bedeutsames Rechtsgut und setzt bei Sachwerten voraus, dass eine Gefahr für nicht unwesentliche Vermögenswerte besteht. Diese Voraussetzung dürfte bei Vorliegen des Verdachts der Verschiebung eines Kfz regelmäßig gegeben sein. Bei einigen der von mir festgestellten Datenübermittlungen war aber nicht ersichtlich, dass die bayerischen Polizeibeamten über ausreichende Informationen verfügten, um diesen Verdacht bejahen zu können. Zumindest waren solche Informationen nicht dokumentiert. Ich habe deshalb gebeten, von Datenübermittlungen künftig Abstand zu nehmen, wenn die Erforderlichkeit nicht **nachvollziehbar begründet** ist. Andernfalls werde ich eine Beanstandung dieser Verfahrensweise prüfen.

Hinzu kommt, dass die Übermittlung der pauschalen Information, der Betroffene sei in polizeilichen Dateien gespeichert, wegen ihrer Undifferenziertheit keine geeignete Grundlage für die Entscheidung der ausländischen Polizei darstellt, ob und ggf. welche Maßnahmen gegen den Betroffenen zu treffen sind. Ganz im Gegenteil besteht für diesen die Gefahr, dass im Zusammenhang mit Kfz-Verschiebung nicht relevante Erkenntnisse zu Fehlentscheidungen der ausländischen Polizei führen. So könnte der Betroffene in polizeilichen Dateien z. B. wegen übler Nachrede oder Beleidigung gespeichert sein. Zur Verdachtsschöpfung bei der Bekämpfung von Kfz-Verschiebungen wäre diese Speicherung zweifellos irrelevant. Aus datenschutzrechtlicher Sicht sollten solche Mitteilungen deshalb unterbleiben. Auch hier werde ich bei Fortsetzung des bisherigen Verfahrens eine Beanstandung prüfen.

5.3.5 Datei „Gruppentypische Aggressionsdelikte / kriminogene Gruppierungen / Skinheads“

Die Datei dient der Informationssammlung, -auswertung und -steuerung, um frühzeitig die Bildung delinquenter Gruppen zu erkennen und die Strafverfolgung und Gefahrenabwehr zu unterstützen. Gespeichert werden können insbesondere Personen, gegen die wegen jugend- oder gruppentypischer Aggressionsdelikte (insbesondere Vandalismus, Körperverletzung, Sittlichkeitsdelikte, Raub und räuberische Erpressung, Tötungsdelikte oder Ordnungswidrigkeiten) ermittelt wurde oder Personen, die aufgrund glaubwürdiger Hinweise oder polizeilicher Ermittlungen gewälttätigen Gruppierungen oder deren engerem Umfeld zuzuordnen sind.
Bei meiner Prüfung der Speicherungen in dieser Datei bei einem Polizeipräsidium habe ich festgestellt, dass fünf Personen gespeichert waren, die von der Polizei der sog. Punkerszene zugeordnet wurden. Nach den Erkenntnissen aus der Datei selbst und der mir zu den Personen vorgelegten Unterlagen waren die von der Errichtungsanordnung vorgegebenen Speicherungskriterien nicht erfüllt. Beispielsweise war eine junge Frau gespeichert, zu der als einzige Erkenntnis ihre Eigenschaft als Geschädigte eines Diebstahls vorlag. Auch bei den anderen „Punkern“ gab es nach meiner Feststellung keine polizeilichen Erkennisse dafür, dass gegen diese wegen jugend- oder gruppentypischer Aggressionsdelikte ermittelt wurde oder dass sie gewalttätigen Gruppierungen oder deren engerem Umfeld zuzuordnen sind.

Ich habe das Polizeipräsidium aufgefordert, die Speicherungen zu löschen, wenn nicht noch Erkenntnisse mitgeteilt werden können, die die Speicherungen in der Datei rechtfertigen. Die Speicherung zu o.g. junger Frau wurde gelöscht. Die Prüfung der zu den anderen Personen nach Redationsschluss mitgeteilten Erkenntnisse ist noch nicht abgeschlossen.

5.3.6 Dateien für den Bereich Prostitution

Dateien für den Bereich der Prostitution werden von Polizeidienststellen vor allem in den Ballungsräumen und in größeren Städten geführt, die ein polizeilich relevantes Prostitutionsmilieu aufweisen. In diesen Dateien werden personenbezogene Daten von Zuhältern oder von Personen die als solche verdächtig sind, von Personen, die zum Prostitutionsgeschehen beitragen, die der verbotenen Prostitution nachgehen aber auch von Prostituierten, welche diese Tätigkeit legal ausüben, gespeichert.

Die polizeiliche Speicherung Prostituierter hat das Staatsministerium des Innern bereits 1993 insbesondere wie folgt begründet:

- Die umfassende Beobachtung der Prostitution sei zur polizeilichen Aufgabenerfüllung der Gefahrenabwehr und Strafverfolgung dringend erforderlich. Prostitution sei wegen der gebotenen Gewinnchancen und der permanenten Auseinandersetzungen um Marktanteile **extrem kriminalitätsfördernd.** Das gelte nicht nur für die mit der Prostitution direkt zusammenhängenden Tatbestände, wie Förderung der Prostitution, Zuhälterei und Menschenhandel, sondern auch für ihre Begleitkriminalität.

- Polizeiliche Aufgabe bei der Beobachtung der Prostitution sei ferner die Mitwirkung bei der Bekämpfung von übertragbaren Krankheiten.

- Darüber hinaus sei festzustellen, dass das Prostitutionsumfeld häufig der „Organisierten Kriminalität“ zugerechnet werden muss.

Die Erforderlichkeit der Speicherung von Prostituierten obliegt im Einzelfall der **fachlichen Beurteilung** der Polizei. In meiner datenschutzrechtlichen Prüfungskompetenz liegt aber die Feststellung, ob sich die fachliche Beurteilung im Rahmen des Vertretbaren hält. Im Hinblick darauf habe ich bisher Bedenken gegen die Führung solcher Dateien im Grundsatz nicht erhoben.

Folgende Mängel bei der Umsetzung im Detail habe ich bei meinen Prüfungen festgestellt:

In der Datei einer Polizeidirektion wurden die Ehemänner von Prostituierten als potenzielle Zuhälter gespeichert. Ausreichende Anhaltspunkte für diese Annahme konnte ich nicht feststellen. Die Tatsache, dass die Ehemänner der Prostituierten arbeitslos bzw. Alkoholiker waren, begründet noch nicht den Verdacht der Zuhälterei. Nach längerer Überzeugungsarbeit bei der speichernden Polizeidienststelle wurden die Speicherungen gelöscht.

Bei einer weiteren Polizeidienststelle habe ich festgestellt, dass die automatische Fristverlängerung (vgl. Nr. 5.3.1.2) auch auf die Speicherungsfristen von Personen ausgedehnt wurde, die nicht Beschuldigte im Rahmen strafrechtlicher Ermittlungsverfahren waren (z.B. Prostituierte, die ihre Tätigkeit legal ausüben). Diesem Verfahren habe ich widersprochen. Eine Speicherungsverlängerung im Rahmen der sog. Mitziehautomatik kommt gem. Art. 38 Abs. 2 Satz 5 PAG nur bei der Speicherung personenbezogener Daten in Betracht, die gem. Art. 38 Abs. 2 Satz 1 PAG im Rahmen strafrechtlicher Ermittlungsverfahren gewonnen wurden oder von Personen, die verdächtig sind, eine Straftat begangen zu haben. Die Speicherung der Daten anderer Personen erfolgt nach Art. 38 Abs. 1 i.V.m. Art. 37 Abs. 3 PAG. Eine Mitziehautomatik sehen diese Vorschriften nicht vor. Ich habe die Polizei aufgefordert, die Errichtungsanordnung entsprechend zu korrigieren. Eine Antwort steht noch aus.

5.3.7 Datei „LAGE B“

Bei einer Polizeidirektion habe ich die Speicherungen in einer Lagedatei „LAGE B“ (vgl. auch Nr. 5.4.1) geprüft.
Ich habe bemängelt, dass ein Teil der in die Datei LAGE B übernommenen Sachverhalte ohne ausreichende Prüfung der Erforderlichkeit über einen vorgegebenen Verteilerschlüssel als täglicher Lagebericht per Fernschreiben an andere Polizeidienststellen übersandt wurde. Neben den nachgeordneten Polizeiinspektionen, dem Polizeipräsidium, benachbarten Polizeidirektionen und der zuständigen Staatsanwaltschaft erhielten auch Polizeidienststellen Baden-Württembergs diesen Lagebericht. Die dabei übermittelten Sachverhalte enthielten zum Teil personenbezogene Daten von Geschädigten und Tatverdächtigen.

Grundsätzlich kann die Polizei nach Art. 40 Abs. 1 Polizeiaufgabengesetz (PAG) personenbezogene Daten an andere Polizeidienststellen übermitteln, soweit dies zur Erfüllung polizeilicher

Aufgaben erforderlich ist. Dies gilt auch für die Datenübermittlungen an Polizeidienststellen anderer Länder oder des Bundes.

Die pauschale Übermittlung personenbezogener Daten über einen vorgegebenen Verteilerschlüssel halte ich jedoch nicht für zulässig, da für jeden Sachverhalt einzeln geprüft werden muss, ob die Datenübermittlung zur polizeilichen Aufgabenerfüllung erforderlich ist. Eine sorgfältige Prüfung, an wen welche personenbezogenen Informationen übermittelt werden dürfen, ist auch deswegen notwendig, weil die übermittelnde Polizeidienststelle keinen Einfluss auf die weitere Verarbeitung dieser Daten durch die Empfängerdienststellen hat und weil offensichtlich auch keine Nachmeldungen, z.B. hinsichtlich des Verfahrensausgangs, erfolgten.

Ich habe die Polizeidienststelle deshalb gebeten, das bisherige Verfahren der pauschalen Datenübermittlung an andere Polizeidienststellen, insbesondere an außerbayerische einzustellen. Die Polizei hat daraufhin ihre bisherige Praxis geändert. Eine pauschale Übermittlung von personenbezogenen Daten an andere Dienststellen erfolgt nicht mehr.

5.4 Überprüfung von Errichtungsanordnungen für Dateien

Im Berichtszeitraum sind mir für meine datenschutzrechtliche Prüfung wiederum zahlreiche Errichtungsanordnungen für polizeiliche Dateien von verschiedenen Polizeipräsidien zugesandt worden. In erster Linie handelte es sich um Errichtungsanordnungen für Dateien zur Gefahrenabwehr und zur Verfolgung von Straftaten und Ordnungswidrigkeiten, sog. GAST-Dateien. Solche Dateien können die Polizeipräsidien innerhalb eines vom Staatsministerium des Innern vorgegebenen Rahmens (sog. Rahmenerrichtungsanordnung) in eigener Zuständigkeit errichten (vgl. 18. Tätigkeitsbericht, Nr. 5.3.5). Bisher waren dies überwiegend sog. deliktsgruppenspezifische Dateien, d.h. Datensammlungen in Bezug auf bestimmte Deliktsbereiche (z.B. organisierte Kriminalität, Fälschungsdelikte, Prostitution etc.) oder Dateien, die der Vereinfachung von Arbeitsabläufen bei einzelnen Polizeidienststellen (z.B. zur Abwicklung umfangreicher Ermittlungsverfahren im Bereich der Wirtschaftskriminalität oder zur Durchführung größerer polizeilicher Einsätze) dienen sollen. Im Rahmen der Errichtungsanordnung für GAST-Dateien wurden mir auch mehrere Errichtungsanordnungen zu sog. Lagedateien (vgl. Nr. 5.4.1) vorgelegt.

Bei vielen Errichtungsanordnungen habe ich - allerdings mit abnehmender Tendenz - wiederum datenschutzrechtliche Defizite festgestellt. Diese betrafen u. a. die unzureichende Festlegung des Dateienzwecks und des zur Speicherung vorgesehenen Personenkreises, die Speicherungs- und Überprüfungsfristen sowie den Umfang der zu speichernden personenbezogenen Daten.

Im Folgenden werde ich auf einzelne Problemfelder der von mir geprüften Errichtungsanordnungen eingehen.

5.4.1 Lage-Dateien

Bei Lage-Dateien handelt es sich um die Sammlung und Zusammenführung in der Regel bereits erhobener polizeirelevanter Informationen zur Erstellung von Lagebildern (aktuelle Sicherheitslage) für einen bestimmten geographischen Raum. Die so gewonnenen und nach bestimmten Kriterien ausgewerteten Erkenntnisse (z.B. Brennpunkte, Entwicklungen, Zusammenhänge) sol-

len der Polizei im Rahmen ihrer Aufgaben Ansätze für künftige strategische, taktische und operative Maßnahmen liefern.

Die Informationen für die Lagedateien kommen auf verschiedenen Wegen, z.B. fernschriftlich, elektronisch oder mittels Generierung aus anderen Dateien (insbesondere aus den regionalen Dateien „Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung - PSV). Die Auswertung erfolgt durch Lagedienste verschiedener hierarchischer Ebenen (z. B. Polizeiinspektion, -direktion und -präsidium).

Der Zugriff auf Lage-Dateien war bisher auf Dienststellen im Rahmen ihrer bereichsspezifischen Aufgaben (z.B. bestimmte Kriminalpolizeiinspektionen oder Kriminalkommissariate) und/oder auf Dienststellen, für deren regional begrenzten örtlichen Zuständigkeitsbereich (z.B. Polizeiinspektions- oder -direktionsebene) beschränkt.

Möglicherweise aufgrund der fortschreitenden technischen Entwicklung bei Datenbanken und der Vernetzung von Rechnern ist nunmehr eine Tendenz zu erkennen, den Kreis der auf Lagedateien Zugriffsberechtigten sowohl in funktioneller als auch in geographischer Hinsicht erheblich zu erweitern, ohne dabei den Zweck einer Lagedatei ausreichend zu berücksichtigen.
So hat mir ein Polizeipräsidium eine Errichtungsanordnung vorgelegt, wonach sämtliche (auch personenbezogene) Lagedaten des Polizeipräsidiums nicht mehr wie bisher den zuständigen Lagediensten, sondern allen bayerischen Polizeibeamten zugänglich gemacht werden sollten.

Abgesehen davon, dass der bayernweite Zugriff auf Präsidiumsdaten von der Rahmenerrichtungsanordnung GAST (vgl. Nr. 5.4) nicht gedeckt wird, halte ich diese Entwicklung insgesamt für bedenklich. Sie ermöglicht unter der Bezeichnung „Lagedatei“ das Entstehen weiterer polizeilicher Informationssysteme neben dem Kriminalaktennachweis (KAN), welche die personenbezogene Recherche bayernweit eröffnen. Während aber im KAN grundsätzlich nur Beschuldigte gespeichert werden, sollen in den Lagedateien auch andere Personengruppen, wie Opfer, Verletzte, Anzeigeerstatter, Mitteiler, Kontaktpersonen und Unfallbeteiligte erfasst werden. Die Speicherung dieser Gruppen war bisher auf die regionalen Vorgangsverwaltungsdateien (PSV) der einzelnen Polizeidienststellen mit regional begrenztem Zugriff beschränkt. Sie sollte nicht auf dem Weg über „Lagedateien“ bayernweit zugänglich werden.

Ich habe die betroffene Polizeidienststelle deshalb aufgefordert mir mitzuteilen, wieso der Zugriff auf diese Daten für **jeden einzelnen Polizeibeamten** zum Zweck der Feststellung und Bewertung der Lage und der Planung und Durchführung polizeilicher Maßnahmen erforderlich und verhältnismäßig sein soll. Auch sollte begründet werden, ob und ggf. weshalb für den Zweck einer Lagedatei (s. o.) die Speicherung von Personendaten erforderlich ist.

Die Stellungnahme der betroffenen Polizeidienststelle steht noch aus.

In meinem 18. Tätigkeitsbericht (vgl. dort Nr. 5.3.5.1) habe ich über die Speicherung personenbezogener Daten von Sinti- und Roma-Gruppen in der Lage-Datei einer Polizeidirektion berichtet. Das Staatsministerium des Innern hat der Polizei die Speicherung in der bisher praktizierten Weise per Anordnung untersagt und das Bayerische Landeskriminalamt beauftragt, die Verwendung des Schlagwortes „ILAN“ (Information über Landfahrer) technisch zu unterbinden. Bei meiner Prüfung einer Polizeidirektion habe ich festgestellt, dass die Untersagung des Innenministeriums durch das verantwortliche Präsidium noch nicht umgesetzt war. Die technische Unterbindung des Schlagwortes „ILAN“ durch das BLKA war aber bereits realisiert wurde.

Das Staatsministerium des Innern hat sich im Übrigen zu meiner Forderung, keine pauschale Speicherung von Sinti- und Roma-Gruppen vorzunehmen, noch nicht abschließend geäußert.

5.4.2 Datei „vorgetäuschte Verkehrsunfälle“

Ein Polizeipräsidium hat mir die Errichtungsanordnung für eine Datei vorgelegt, deren Zweck es sein soll, durch Sammlung, Auswertung und Zusammenführung polizeilich relevanter Erkenntnisse Straftaten im Bereich vorgetäuschter Verkehrsunfälle zu verhüten und aufzuklären. In diesem Zusammenhang sollten auch Rechtsanwälte gespeichert werden, die Tatverdächtige bei der Durchsetzung von Forderungen im Rahmen der Schadensregulierung vertreten. Ich habe das Polizeipräsidium darauf hingewiesen, dass ich eine Speicherung von Rechtsanwälten, die Organe der Rechtspflege sind, als potenziell Verdächtige alleine wegen ihrer anwaltschaftlichen Vertretung nicht für gerechtfertigt halte. Das Polizeipräsidium hat mir daraufhin eine Neufassung der Errichtungsanordnung vorgelegt, bei der jedoch weiterhin die Speicherung von Rechtsanwälten vorgesehen war. Nach den dort gewählten Formulierungen sollen Rechtsanwälte nur dann in der

Datei gespeichert werden, wenn sie als Tatverdächtige in Frage kommen. Für diesen Fall bestehen aus meiner Sicht gegen eine Speicherung ebenso wenig Bedenken wie gegen die eines anderen Tatverdächtigen. Dafür bedarf es aber keiner gesonderten Kategorie.

Das Polizeipräsidium hat mir dann mitgeteilt, dass die gesonderte Speicherung von Rechtsanwälten in dieser Datei unterbleibt.

5.5 Beteiligung des Datenschutzbeauftragten an Errichtungsanordnungen für Verbunddateien des polizeilichen Informationssystems INPOL

Nach § 34 Abs. 1 Bundeskriminalamtgesetz (BKAG) hat das Bundeskriminalamt (BKA) für jede bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten in einer Errichtungsanordnung u. a. Zweck, betroffener Personenkreis, Art der zu speichernden Daten und Speicherungsdauer festzulegen. Diese Errichtungsanordnung bedarf der Zustimmung des Bundesministeriums des Innern. Nach Abs. 2 dieser Vorschrift bedarf die Errichtungsanordnung bei Dateien des polizeilichen Informationssystems (Verbunddateien) auch der Zustimmung der zuständigen Innenministerien und Senatsinnenverwaltungen der Länder. Vor der Entscheidung sind die Landesbeauftragten für den Datenschutz zu informieren. Nach dem bisherigen Verfahren wurden dazu die Entwürfe der Errichtungsanordnungen für neue Verbunddateien vom Bundesministerium des Innern den Landesinnenressorts und von diesen den jeweiligen Landesbeauftragten übersandt.

Aufgrund einer in der Vergangenheit teilweise nicht rechtzeitigen Beteiligung von Landesbeauftragten war das Bundesinnenministerium grundsätzlich bereit, gleichzeitig mit dem Versand der Entwurfsfassung der Errichtungsanordnungen an die Innenverwaltungen der Länder auch den Landesbeauftragten einen Abdruck zu übersenden. Es machte eine derartige Verfahrensweise jedoch von der Zustimmung sämtlicher Innenministerien der Länder abhängig. Das Bayerische Staatsministerium des Innern stimmte dieser Verfahrensweise zunächst nicht zu.

Ich habe das Staatsministerium des Innern wiederholt gebeten, dem Vorschlag des Bundesinnenministeriums für eine unmittelbare Beteiligung der Landesdatenschutzbeauftragten zuzustimmen, und darauf hingewiesen, dass ich das geplante Verfahren einer unmittelbaren Beteiligung im Rahmen des § 34 Abs. 1 und 2 BKAG auch aus arbeitsökonomischen Gründen für sinnvoll halte. Für das Staatsministerium des Innern würde sich dadurch die unverzügliche Weiterleitung der Entwurfsfassungen für Errichtungsanordnungen an mich erübrigen. Für meine Behörde ergäbe sich daraus der Vorteil einer noch frühzeitigeren Beteiligung am Verfahren. Ich habe das Innenministerium darauf aufmerksam gemacht, dass die zentrale Unterrichtung aller Landesdatenschutzbeauftragten zuletzt allein an seiner ablehnenden Haltung zu scheitern drohe, und anhand von Beispielen darauf hingewiesen, dass meine Beteiligung durch das Innenministe-

rium in der Vergangenheit nicht stets im erforderlichen Maße gewährleistet war (vgl. hierzu Nr. 5.10).

Das Innenministerium hat der vorgeschlagenen Verfahrensweise schließlich zugestimmt.

5.5.1 INPOL-Neukonzeption

Die Polizeien des Bundes und der Länder verarbeiten zentral in großem Umfang personenbezogene Daten, um einen schnellen und effektiven Austausch von Informationen zu gewährleisten. Beim Bundeskriminalamt (BKA) wird dazu das bundesweite polizeiliche Informationssystem INPOL geführt. Seit dem 01.10.1996 arbeitet beim BKA eine aus mittlerweile ca. 130 Mitarbeitern bestehende Projektgruppe an einem neuen, erweiterten Konzept für dieses System. Bei dieser INPOL-neu genannten Neukonzeption handelt es sich nicht lediglich um eine bloße Fortentwicklung, sondern um eine grundlegende Neustrukturierung des bestehenden polizeilichen Informationssystems. Anlass für die Neukonzeption sind neben dem Interesse, moderne technische Möglichkeiten auch für die Polizei nutzbar zu machen, insbesondere auch veränderte Bedürfnisse, die aus polizeifachlicher Sicht zur Bewältigung des immer komplexer werdenden Informationsaufkommens bestehen. Für die datenschutzrechtliche Kontrolle des Projekts haben die Datenschutzbeauftragten des Bundes und der Länder eine eigene Arbeitsgruppe gebildet, die auch über laufende Teilprojekte informiert wird. Diese externe Begleitung des Projekts durch die Datenschutzbeauftragten wird jedoch durch die abschnittsweise Entwicklung des Projekts vor erhebliche Schwierigkeiten gestellt. Probleme ergeben sich auch aus der Tatsache, dass es sich bei INPOL-neu um eine Verbundanwendung für Daten aller Länderpolizeien handelt, die jedenfalls nach Meinung der Landesbeauftragten für den Datenschutz aufgrund der verschiedenen Landespolizeigesetze unterschiedlichen Vorschriften unterliegen.

Kernpunkt von INPOL-neu ist die Errichtung eines einheitlichen, anwendungsunabhängigen Datenbestandes. Nach diesem Konzept sollen alle Erkenntnisse zu einer Person lediglich einmal in die Datenbank eingegeben werden. Je nach dem Zweck späterer Abfragen sollen dann lediglich einzelne oder umfassende Informationen zu einer Person ausgegeben werden. Demgegenüber sind beim gegenwärtigen Informationsverbund die Datenbestände grundsätzlich getrennt. Da die datenschutzrechtlichen Grundprinzipien der Zweckbindung und der Erforderlichkeit ei-

nen uneingeschränkten Zugriff jedes polizeilichen Nutzers auf sämtliche in INPOL-neu erfassten personenbezogenen Daten nicht zulassen, sollen über ein komplexes Berechtigungssystem unterschiedliche Zugriffsmöglichkeiten auf die Daten geschaffen werden.

Einige der angestrebten Teilkonzepte halte ich mit den gesetzlichen Ermächtigungsnormen im Bundeskriminalamtgesetz (BKAG) nur für schwer vereinbar. So sollen etwa - abweichend vom gegenwärtigen Verfahren - in den bundesweiten KAN (vgl. Nr. 5.3.1) bei Vorliegen einer INPOL-relevanten Straftat auch solche Taten eines Beschuldigen aufgenommen werden, die für sich genommen keine länderübergreifende oder erhebliche Bedeutung aufweisen. Die Datenschutzbeauftragten des Bundes und der Länder haben auf die rechtliche Unzulässigkeit der Aufnahme der sog. kriminellen Historie in den Bundes-KAN hingewiesen.

Im Rahmen der Neukonzeption wird von zahlreichen Ländern, darunter auch von Bayern, angestrebt, ihre polizeilichen Daten im Wege der Auftragsdatenverarbeitung an das BKA auszulagern. Eine solche Datenverarbeitung des BKA war für die Länder zunächst nur für eine Übergangsfrist vorgesehen. Mittlerweile haben die betreffenden Länder jedoch überwiegend zu erkennen gegeben, dass sie eine dauerhafte Verarbeitung Ihrer polizeilichen Daten beim BKA wollen. Auch das Bundesministerium des Innern hat sich dahin gehend geäußert, dass eine derartige dauerhafte Lösung wirtschaftlich erstrebenswert und technisch sowie rechtlich möglich sei. Die Datenschutzbeauftragten des Bundes und der Länder sind mit mir dieser Haltung entgegengetreten. Besonders bereitet die Erwartung Sorge, dass die zentrale Speicherung der jeweiligen Länderdaten beim BKA über kurz oder lang eine Aufweichung der nach dem Gesetz erforderlichen strikten Trennung der unterschiedlichen Datenbestände des Bundes und der Länder begünstigt. Forderungen, polizeiliche Erkenntnisse verschiedener Länder zur selben Person dem Zugriff anderer Länder zu öffnen, wurden bereits erhoben. Es muss jedoch auch bei einer Auftragsdatenverarbeitung sichergestellt sein, dass jedes Land grundsätzlich nur die Daten aus dem landeseigenen Datenbestand nutzen kann.

Wegen seiner beträchtlichen Auswirkungen auf die Möglichkeiten der polizeilichen Datenverarbeitung bedarf das Projekt INPOL-neu auch weiterhin der großen Aufmerksamkeit der Datenschutzbeauftragten.

5.5.2 Fristberechnung bei der retrograden Speicherung von DNA-Profilen in der DNA-Analyse-Datei

In meinem letzten Tätigkeitsbericht hatte ich über die Errichtung einer zentralen DNA-Analyse-Datei berichtet (Nr. 7.1.7) und ausgeführt, dass Erhebung und Speicherung der betreffenden Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren erfolgen. In diese neu errichtete Datei werden auch die DNA-Identifizierungsmuster von Personen aufgenommen, die bereits wegen Straftaten von erheblicher Bedeutung verurteilt worden sind (sog. Retrograderfassung, näheres hierzu unter Nr. 7.2.3.1).

Anlässlich meiner datenschutzrechtlichen Prüfung bei einer Polizeidirektion habe ich Kenntnis von Schreiben des Innenministeriums und des Bayerischen Landeskriminalamts (BLKA) erhalten, in welchen wichtige Grundsätze für diese Speicherungen aufgestellt werden.

So stellt das BLKA fest, dass die Festlegung der Aussonderungsprüffrist in der DNA-Analyse-Datei, die auch die Eingabe einer Speicherungsfrist von mehr als zehn Jahren erlaube, grundsätzlich an die des Kriminalaktennachweises (vgl. Nr. 5.3.1.3) gebunden sei, in dem bei bestimmten Sexualdelikten Aussonderungsprüffristen von 20 Jahren vergeben worden seien.

Die vom BLKA angesprochene Vergabe einer mehr als zehnjährigen Speicherungsprüffrist in der DNA-Analyse-Datei halte ich nicht mit dem Gesetz für vereinbar. Unabhängig von der Frage der Zulassung längerer als 10-jähriger Speicherungsprüffristen im Kriminalaktennachweis der Bayerischen Polizei durch das Polizeiaufgabengesetz (etwa bei Sexualstraftaten), ist eine entsprechende Fristenvergabe in der DNA-Analyse-Datei schon aufgrund der bundesrechtlichen Regelung in § 32 Abs. 3 Satz 2 Bundeskriminalamtgesetz (BKAG) nicht möglich. Danach dürfen die festzulegenden Aussonderungsprüffristen bei Erwachsenen zehn Jahre, bei Jugendlichen fünf und bei Kindern zwei Jahre nicht überschreiten (so auch die Errichtungsanordnung zur DNA-Analyse-Datei). Maßgeblich für Speicherumfang und -fristen in polizeilichen Verbunddateien sind zwar grundsätzlich die Regelungen in den Landespolizeigesetzen. Das BKAG ist jedoch in dem Sinne entscheidend, als es jedenfalls eine Obergrenze für die Zulässigkeit der Speicherungen darstellt.

Ich habe das Staatsministerium des Innern gebeten, die entsprechende Regelung im Schreiben des BLKA aufzuheben und etwaige Prüffristen, die über die Höchstfristen des BKAG hinausgehen, zu berichtigen.

Das Staatsministerium des Innern hat hierauf mittlerweile zustimmend geantwortet, dass auch aus seiner Sicht die Vorschrift des § 32 Abs. 3 BKAG auch für die von Bayern in die Verbundanwendung angelieferten Datensätze gelte. Das BLKA werde hierzu eine ergänzende Klarstellung für die Dienststellen der Bayerischen Polizei veranlassen.

5.5.3 Automatisches Fingerabdruck-Identifizierungssystem-AFIS

In meinem 17. Tätigkeitsbericht (Nr. 5.3.1) hatte ich über das beim Bundeskriminalamt (BKA) betriebene automatische Fingerabdruck-Identifizierungssystem (AFIS) berichtet, das für Zwecke der Kriminalitätsbekämpfung bereits seit Ende 1993 ohne Errichtungsanordnung auf der Grundlage einer sogenannten Sofortanordnung des BKA genutzt wird.

Mittlerweile liegt der Entwurf einer Errichtungsanordnung für die sog. Datei AFIS-P des Bundesministeriums des Innern vor, dem das Staatsministerium des Innern zugestimmt hat. Es hat in diesem Zusammenhang den Standpunkt vertreten, dass die Aussonderungsprüffrist nach bayerischem Landesrecht im Zusammenhang mit Sexualstraftaten und Gewaltdelikten mit sexuellem Hintergrund in der Regel 20 Jahre betrage. Aus diesem Grunde werde bei den vorgenannten Deliktsbereichen die Aussonderungsprüffrist bei bayerischen AFIS-Speicherungen regelmäßig auf 20 Jahre verlängert. Für den Bereich aller sonstigen Delikte hat das Innenministerium das BLKA um Prüfung des Vorhabens gebeten, eine Aussonderungsprüfung erst nach 15 Jahren vorzusehen.

Hierzu ist festzustellen, dass die Vergabe einer mehr als 10-jährigen Aussonderungsprüffrist mit der im Entwurf der Errichtungsanordnung enthaltenen Höchstfrist nicht vereinbar ist. Insbesondere aber legt die Vorschrift des § 32 Abs. 3 Satz 2 Bundeskriminalamtgesetz (BKAG) fest, dass die Aussonderungsprüffristen bei Erwachsenen 10 Jahre nicht überschreiten dürfen. Diese Höchstfrist des BKAG ist auch für bayerische AFIS-Speicherungen maßgeblich.

Ich habe das Innenministerium auf die Rechtslage hingewiesen und hierzu um Stellungnahme gebeten. Das Innenministerium hat eingeräumt, dass für die angestrebte Verlängerung der Speicherungsprüffristen eine Gesetzesänderung notwendig wäre. Längere als 10-jährige Aussonderungsprüffristen würden nicht vergeben.

5.6 Kontrolle von Datenerhebungsmaßnahmen

5.6.1 Verdachts- und ereignisunabhängige Kontrollen

In meinen letzten Tätigkeitsberichten hatte ich die in Art. 13 Abs. 1 Nr. 5 Polizeiaufgabengesetz (PAG) geschaffene erweiterte Möglichkeit zur Durchführung verdachts- und ereignisunabhängiger polizeilicher Kontrollen dargestellt. Zuletzt hatte ich berichtet (vgl. 18. Tätigkeitsbericht, Nr. 5.5.1), dass schriftliche Anfragen beim Innenministerium und verschiedenen Polizeidienststellen sowie mehrere Informationsbesuche auch bei örtlichen Dienststellen bestätigt hatten, dass nach wie vor bei den Polizeidienststellen keine Übersicht über die durchgeführten verdachts- und ereignisunabhängigen Kontrollen und deren Erfolge besteht, so dass im Nachhinein weder die Anzahl der Kontrollmaßnahmen feststellbar, noch deren rechtliche Einordnung möglich ist. Offenbar werden nur herausragende Ereignisse an vorgesetzte Dienststellen gemeldet.

Gegen die Erweiterung der polizeilichen Befugnisse zur Identitätsfeststellung habe ich mich nicht grundsätzlich ausgesprochen. Bereits während des Gesetzgebungsverfahrens hatte ich aber Einschränkungen dahin gehend gefordert, die Befugnis der Polizei zur Identitätsfeststellung auf Durchgangsstraßen nur zur Bekämpfung der grenzüberschreitenden Kriminalität von **erheblicher** Bedeutung einzusetzen. Außerhalb von Bundesautobahnen und Europastraßen sollte der Einsatz auf den im Gesetz genannten „anderen Straßen von erheblicher Bedeutung für den grenzüberschreitenden Verkehr“ angesichts der sehr weiten Fassung des Gesetzestextes nur auf der Grundlage einer **Lagebeurteilung** und einer **zeitlich befristeten Anordnung** durch den Leiter der polizeilichen Führungsdienststelle erfolgen. Meine Forderungen wurden nicht aufgegriffen.

Mittlerweile hat das Landesverfassungsgericht Mecklenburg-Vorpommern mit Urteil vom 21.10.1999 entschieden, dass die vergleichbare dortige gesetzliche Regelung überwiegend verfassungswidrig und nichtig ist. Auf der Grundlage der vom Gericht überprüften Regelung ist es der Polizei in Mecklenburg-Vorpommern derzeit nicht gestattet, auf Durchgangsstraßen außerhalb des 30 Kilometer tiefen Grenzgebietes Personen ohne konkreten Anlass zu kontrollieren. Darüber hinaus darf sie im Grenzgebiet bis zu einer Tiefe von 30 Kilometern, in Einrichtungen des internationalen Verkehrs und im Küstenmeer künftig Personen lediglich nur noch anhalten

und diese nach den Ausweispapieren fragen. Weiter gehende Zwangsmaßnahmen wie etwa das Verbringen zur Dienststelle, die Durchsuchung der Person und ihrer Sachen sowie die Verarbeitung und Nutzung der dabei anfallenden personenbezogenen Daten hat das Verfassungsgericht für nicht zulässig gehalten. In den Urteilsgründen führt das Gericht u.a. aus, dass „der Gesetzgeber Eingriffsschwellen festlegen“ muss, „etwa indem er darauf abstellt, dass nach Lage, Erkenntnissen und polizeilicher Erfahrung sich auf einer Durchgangsstraße grenzüberschreitende organisierte Kriminalität abzeichnet“.

Ich habe mich an den Staatsminister des Innern mit der Bitte gewandt, diese Verfassungsgerichtsentscheidung zum Anlass für eine nochmalige Überprüfung der bayerischen Regelung zu nehmen. Bei dieser Gelegenheit habe ich erneut darauf hingewiesen, dass ich es nach wie vor für erforderlich halte, dass durch geeignete Maßnahmen Erforderlichkeit und Wirksamkeit der verdachtsunabhängigen Kontrollen überprüft werden (Evaluierung).

Der Innenminister hat mir hierzu mitgeteilt, dass aufgrund des Urteils derzeit kein Anlass bestünde, die geltende bayerische Regelung zur Schleierfahndung zu ändern. Die von mir geforderte Evaluierung verursache einen unvertretbar hohen Verwaltungsaufwand. Die betreffenden Kontrollen seien einer einheitlichen statistischen Auswertung nur schwer zugänglich.

Da es dem Innenministerium trotz der von ihm gesehenen Schwierigkeiten möglich ist, auf Erfolgsbilanzen dieser polizeilichen Kontrollbefugnis zu verweisen, sollte auch eine ausreichende Unterrichtung z. B. des Landesbeauftragten für den Datenschutz über Zahl und Ort der getroffenen Maßnahmen sowie ihre Ergebnisse möglich sein. So ist etwa im neuen Sächsischen Polizeigesetz vorgesehen, dass das dortige Innenministerium den Umfang und die Ergebnisse der Anwendung der verdachtsunabhängigen polizeilichen Kontrollen erfasst und hierüber jährlich dem Sächsischen Datenschutzbeauftragten berichtet. Auch der Deutsche Bundestag hat die Bundesregierung gebeten, eine Evaluation des Bundesgrenzschutzgesetzes vorzulegen, obwohl im Gegensatz zur bayerischen Gesetzeslage die dortige Befugnis zur verdachtslosen Personenkontrolle weniger weit geht: Sie umfasst nicht auch die Möglichkeit der Durchsuchung der Betroffenen. Mit der Evaluation erfolgt auch in diesem Bereich eine ständige begleitende Bewertung der Eingriffsbefugnis. Was beim Bund möglich ist, sollte auch in Bayern möglich sein.

5.6.2 Telefonüberwachungsmaßnahmen

Auch in diesem Berichtszeitraum habe ich wieder das Verfahren bei Telefonüberwachungsmaßnahmen sowohl anlassunabhängig als auch aufgrund von Bürgereingaben geprüft. In meinem 18. Tätigkeitsbericht (vgl. Nr. 5.5.3) hatte ich anlässlich meiner Prüfung einer Polizeidienststelle Kritik geäussert an der unzureichenden Dokumentation der Anfertigung von etwaigen Tonbandabschriften oder von Aufzeichnungen über Verbindungsdaten, die bei Telefonüberwachungsmaßnahmen gewonnen wurden. Ich hatte das zuständige Polizeipräsidium aufgefordert, eine ausreichende Dokumentation über Art und Anzahl der durch die Maßnahme gewonnenen Unterlagen, deren Verbleib sowie die Durchführung und den Zeitpunkt der Vernichtung, sicherzustellen. Das Polizeipräsidium hat mir zwischenzeitlich eine Dienstanweisung vorgelegt, in der meine Forderungen in vollem Umfang berücksichtigt wurden. Meine Prüfungen in diesem Berichtszeitraum haben im Übrigen zu keinen negativen Feststellungen geführt.

5.6.3 Bildaufnahmen bei Versammlungen

In meinem letzten Tätigkeitsbericht (Nr. 5.5.7) bin ich auf die Bedeutung einer effektiven datenschutzrechtlichen Kontrolle in dem äußerst sensiblen Grenzbereich zwischen möglichst unbeeinträchtigter Wahrnehmung des Grundrechts auf Demonstrationsfreiheit und notwendiger polizeilicher Aufgabenerfüllung eingegangen.

Meine damalige Bitte an das Staatsministerium des Innern, in Zukunft bei Versammlungen angefertigte polizeiliche Bildaufnahmen zum Zwecke der datenschutzrechtlichen Kontrolle zunächst aufzubewahren und mich hiervon umgehend zu unterrichten, war leider erfolglos. Ich hatte diese Bitte gestellt, um mir eine Kontrolle des angefertigten Bildmaterials zu ermöglichen.

Das Innenministerium wies zunächst darauf hin, dass die erbetene Aufbewahrung und Benachrichtigung von allen angefertigten Bildaufnahmen zu einem erheblichen Meldeaufkommen und einer erheblichen haushaltsmäßigen Mehrbelastung der Polizeidienststellen führen würde.

Darauf bat ich darum, dass mich die Polizeidienststellen im Bereich eines Polizeipräsidiums über die in einem begrenzten Zeitraum angefertigten polizeilichen Bildaufnahmen umgehend unterrichten und dass sie die Aufnahmen bis zu einer entsprechenden Freigabe durch mich zur Datenschutzkontrolle weiter aufbewahren.
Das Innenministerium sagte mir eine entsprechende Verfahrensweise zunächst zu, teilte mir dann aber später mit, dass in dieser Zeit im Bereich dieses Polizeipräsidiums im Gegensatz zu den Bereichen anderer Präsidien keine Bildaufnahmen angefertigt wurden.

In diesem Verfahrensablauf sehe ich keine ausreichende Unterstützung durch das Innenministerium. Ohne diese Unterstützung wird es aber kaum möglich sein, eine effektive Kontrolle polizeilicher Videoaufnahmen sicherzustellen.

Im Berichtszeitraum habe ich im Rahmen einer anderweitigen Datenschutzkontrolle Bildaufzeichnungen geprüft, die die Polizei anlässlich einer Großdemonstration (Wehrmachtsausstellung in München) von Versammlungsteilnehmern und Gegendemonstranten angefertigt hatte. Ich habe die Gelegenheit genutzt, die Polizei anhand des konkreten Vorganges erneut auf die Rechtslage bei Anfertigung von Bildaufnahmen und –aufzeichnungen bei Versammlungen hinzuweisen.

Nach wohl überwiegender Auffassung sind Übersichtsaufnahmen, die zur Leitung des polizeilichen Einsatzes, zu Schulungszwecken oder zur Einsatzdokumentation benötigt und nicht mit dem Ziel hergestellt werden, einzelne Teilnehmer einer Versammlung zu identifizieren, auch ohne gesetzliche Befugnisnorm zulässig (vgl. hierzu auch 16. Tätigkeitsbericht Nr. 5.15). Solche Aufnahmen werden deshalb von mir nicht beanstandet.

Die meiner Prüfung zugrundeliegenden Aufzeichnungen konnten nicht als Übersichtsaufnahmen angesehen werden, weil viele der Einstellungen die Identifizierung eines großen Teils der abgebildeten Personen ermöglichten und mehrfach der Bildausschnitt eigens durch Zoomen auf einzelne Betroffene verengt wurde.

Soweit nach dem Vorbringen der Polizei durch die Bildaufzeichnungen zum Zwecke der Strafverfolgung von Anfang an strafrechtlich relevante Sachverhalte beweissicher festgehalten wer-

den sollten, war anzumerken, dass derartige polizeiliche Maßnahmen nach der Strafprozessordnung den **Anfangsverdacht einer Straftat** voraussetzen. Es müssen grundsätzlich **hinsichtlich jedes Betroffenen** bereits zureichende tatsächliche Anhaltspunkte für bereits begangene oder gerade in Ausführung befindliche Straftaten vorliegen. Die **vorsorgliche Anfertigung** von Bildaufnahmen einer Vielzahl von Personen **wegen zu erwartender Straftaten** ist nach der Strafprozessordnung auch dann nicht zulässig, wenn aufgrund konkreter Hinweise mit Straftaten zu rechnen ist. Diese rechtlichen Voraussetzungen lagen nicht vor.
Bei gewalttätig verlaufenden Versammlungen wird regelmäßig eine „Gemengelage“ anzunehmen sein, die Anlass für polizeiliche Maßnahmen sowohl zur präventiven Gefahrenabwehr als auch zur repressiven Strafverfolgung bietet. Nach herrschender Rechtsprechung ist bei solchen Sachverhalten darauf abzustellen, auf welcher Seite das **Schwergewicht der Maßnahme** liegt. Eine präventivpolizeiliche Maßnahme ist anzunehmen, wenn diese aus objektiver Sicht überwiegend gefahrenabwehrenden Zwecken dient. In dem meiner Prüfung zugrundeliegenden Fall war es vertretbar anzunehmen, dass im Vordergrund die Abwehr der durch Straftaten zu erwartenden erheblichen Gefahren für die öffentliche Sicherheit stand.

Wie ich bereits in meinem 17. Tätigkeitsbericht (Nr. 5.9.1) dargestellt habe, sind Rechtsgrundlagen für die Anfertigung polizeilicher Bildaufnahmen und –aufzeichnungen zur Gefahrenabwehr bei oder im Zusammenhang mit öffentlichen Versammlungen die §§ 12 a, 19 a Versammlungsgesetz (VersammlG). Nach § 12 a VersammlG kann die Polizei Bildaufnahmen von Teilnehmern anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass **von ihnen** erhebliche Gefahren ausgehen. Einzelne Versammlungsteilnehmer dürfen dann gezielt beobachtet werden, wenn man aufgrund ihres Verhaltens oder aufgrund sonstiger Erkenntnisse mit erheblichen Störungen gerade durch diese Teilnehmer rechnen muss und wenn eine solche Beobachtung unter Berücksichtigung des Grundrechts der Versammlungsfreiheit zur Abwehr der bevorstehenden Störung der öffentlichen Sicherheit und Ordnung erforderlich und verhältnismäßig ist.

Kommt die Polizei aufgrund einer **umfassenden Einzelfallprüfung** zu der Erkenntnis, dass im Zusammenhang mit der geplanten Versammlung erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung bevorstehen, ist zu prüfen, welche Personen zum Kreis der potenziellen Störer gehören. Können einzelne Personen als potenzielle Störer identifiziert werden, dürfen von diesen Personen Bild- und Tonaufzeichnungen gemacht werden. Bei Veranstaltungen **homogener**

Gruppierungen kann **je nach den Umständen** die Annahme gerechtfertigt sein, dass **von allen Teilnehmern** eine erhebliche Gefahr ausgeht. Die Annahme einer homogenen Gruppe kann sich auf Erkenntnisse über die Versammlungsteilnehmer, das Thema bzw. Ziel der Veranstaltung und die Person des Veranstalters stützen. Bei solchen Gruppen ist eine individualisierte Gefahrenprognose als Voraussetzung für die Anfertigung von Bild- und Tonaufnahmen nicht erforderlich.

Hiervon zu unterscheiden ist jedoch die Vielzahl von Veranstaltungen, an denen neben friedlichen Teilnehmern nach Erkenntnissen der Polizei auch nicht identifizierte gewaltbereite Personen teilnehmen, von denen erhebliche Gefahren ausgehen. **Die Anfertigung von Bild- und Tonaufnahmen auch der friedlichen Versammlungsteilnehmer ist in diesem Fall nicht von § 12 a VersammlG gedeckt.**

Ob in dem von mir geprüften Fall die von den Bildaufzeichnungen in individualisierbarer Weise betroffenen Personen nach polizeilichen Erkenntnissen jeweils homogenen Gruppierungen im beschriebenen Sinne angehörten oder nur als Dritte unvermeidbar betroffen waren (vgl. § 12 a Abs. 1 Satz 2 VersammlG), war für mich aufgrund der fehlenden objektiven Zuordnungsmöglichkeit nicht mehr abschließend feststellbar.

Ich habe die Polizei gebeten, die dargestellten rechtlichen Voraussetzungen im Rahmen polizeilicher Bildaufnahmen bei Versammlungen zu berücksichtigen.

5.6.4 Videoüberwachung öffentlicher Straßen und Plätze

Von privaten Unternehmen ist der Einsatz von Videotechnik bereits seit langem bekannt, z.B. in Kaufhäusern, Banken und Tankstellen. Die bayerische Polizei nutzte diese Technik im Bereich der Gefahrenabwehr auf öffentlichen Straßen und Plätzen bislang hauptsächlich zur Verkehrsüberwachung, zum Objektschutz oder bei großen Veranstaltungen (z. B. Fußballspielen). Seit einiger Zeit bestehen Überlegungen, Videotechnik gezielt zum Zwecke der vorbeugenden Verbrechensbekämpfung einzusetzen. Hierdurch sollen potenzielle Straftäter abgeschreckt und das Sicherheitsgefühl der Bürger gestärkt werden.

Für die Videobeobachtung im öffentlichen Raum halte ich die Schaffung sicherer Beurteilungskriterien durch eingrenzende gesetzliche Regelungen für erforderlich. Hinsichtlich der datenschutzrechtlichen Anforderungen an solche Regelungen hat die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 eine Entschließung zu „Risiken und Grenzen der Videoüberwachung“ gefasst (vgl. Anlage Nr. 20). Danach müssen eine strenge Zweckbindung, eine Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen, die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen, die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten und die Löschung der Daten binnen kurzer Fristen sichergestellt werden. Unter diesen Voraussetzungen hat die Konferenz die Beobachtung einzelner öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, als denkbaren Einsatz der Videobeobachtung angesehen.
Die grundsätzliche Notwendigkeit einer solchen gesetzlichen Regelung gilt auch dann, wenn die Kameras nur in konkreten Gefahrensituationen oder bei Verdacht auf strafbare Handlungen personenbezogene Aufnahmen machen sollen. Der Bürger, der über sich eine Videokamera sieht, weiß nicht, ob sie ihn aufnimmt oder nicht. Damit berührt ihn die bloße Existenz der Kamera in seiner Freiheitsphäre. Eine gesetzliche Regelung über die Voraussetzungen der Videobeobachtung ist deshalb dringend notwendig. Zu den konkreten Projekten habe ich Folgendes festgestellt:

Der Staatsminister des Innern hat die PD Regensburg beauftragt, ein entsprechendes Pilotprojekt durchzuführen und über die hierbei gewonnenen Erfahrungen zu berichten. Anschließend soll

entschieden werden, inwieweit dieses Pilotprojekt auf andere bayerische Städte ausgedehnt werden kann und inwieweit eine Erweiterung der bestehenden Rechtsvorschriften des Polizeiaufgabengesetzes angezeigt ist.

Ich habe mich bereits vor dem im Frühjahr 2000 erfolgten Start dieses Projekts vor Ort über die tatsächlichen Gegebenheiten und technischen Einrichtungen informiert. Dabei habe ich festgestellt, dass an 7 Plätzen die Bilder von dort bereits bisher vorhandenen, erkennbar angebrachten Kameras der öffentlichen Verkehrsbetriebe in die polizeiliche Einsatzzentrale überspielt werden. Die betreffenden Plätze stellen nach Angabe des Innenministeriums „Angsträume“ dar, an denen sich die Bevölkerung besonders unsicher fühle und/oder die durch ein hohes Kriminalitätsaufkommen aufgefallen seien. Die Polizei hat vorgetragen, dass ein „Zoomen“ der Kameras zur identifizierbaren Beobachtung einzelner Personen und eine Bildaufzeichnung nur bei konkreten Gefahrenlagen oder Straftatverdacht erfolgen würde.

Ich habe das Innenministerium darauf hingewiesen, dass eine Videoüberwachung auch von Örtlichkeiten, an denen Unsicherheitsgefühle der Bevölkerung bestehen, die nicht auch durch objektive Anhaltspunkte für die zukünftige Begehung von Straftaten gestützt werden, problematisch ist. Bei diesen Örtlichkeiten handelt es sich nicht um Kriminalitätsschwerpunkte, für die ich im Einzelfall eine Videoüberwachung für vertretbar halte (abgesehen von der grundsätzlich bestehenden Notwendigkeit einer gesetzlichen Regelung). Ich habe um Stellungnahme gebeten, inwieweit an den vom o.g. Pilotprojekt erfassten Plätzen derartige Anhaltspunkte vorliegen. Das Innenministerium hat mir zwischenzeitlich solche mitgeteilt, die ich im Einzelnen noch überprüfen werde.

In der Presse war ferner über Pläne der Münchner Polizei berichtet worden, die polizeiliche Videoüberwachung erheblich auszuweiten. So werde etwa ein Zugriff der Polizei auf die von der Deutschen Bahn AG im Hauptbahnhof und von der Münchner-U-Bahn-Bewachungsgesellschaft im U-Bahn-Bereich betriebenen Videokameras angestrebt.

Zur Videoüberwachung am Hauptbahnhof hat mir das Innenministerium mitgeteilt, dass eine Mitbenutzung der Videokameras lediglich beabsichtigt und derzeit noch nicht in Betrieb sei. Hinsichtlich der Überwachung im U-Bahn-Bereich hat es ausgeführt, dass die Polizei eine Mit-

benutzung des Videosystems unter einsatztaktischen Gesichtspunkten (bei Unglücksfällen oder im Rahmen der polizeilichen Fahndung nach einem Straftäter, der sich in die U-Bahn-Geschosse geflüchtet hat) plane. Gegen eine solche anlassbezogene polizeiliche Videoüberwachung habe ich im Einzelfall keine grundsätzlichen datenschutzrechtlichen Bedenken.

Gegenwärtig ist die polizeiliche Videoüberwachung im Polizeiaufgabengesetz – abgesehen vom verdeckten Einsatz zu Observationszwecken in Art. 33 Abs. 1 Nr. 2 – ausdrücklich lediglich in Art. 32 Abs.1 bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen sowie in Abs. 2 zu Zwecken des Schutzes gefährdeter Objekte geregelt. Im Zusammenhang mit öffentlichen Versammlungen ist die polizeiliche Anfertigung von Bildaufnahmen in den §§ 12 a und 19 a des Versammlungsgesetzes abschließend geregelt. Eine ausdrückliche Regelung der polizeilichen Videoüberwachung des öffentlichen Raumes im Übrigen fehlt hingegen.

Übergangsweise können wie bemerkt einzelne Videokameras (Übersichtsaufnahmen) an Straßen und Plätzen, bei denen nach der polizeilichen Erfahrung und Lageeinschätzung tatsächliche Anhaltspunkte für die zukünftige Begehung von Straftaten vorliegen (sog. Kriminalitätsschwerpunkte), datenschutzrechtlich hingenommen werden. Eine **flächendeckende Beobachtungsmöglichkeit** hielte ich allerdings aus verfassungsrechtlichen Gründen für **unzulässig**, weil sie den Bürger unter einen ständigen Anpassungsdruck setzen würde. Dieser Druck beeinträchtigt die freie Entfaltungsmöglichkeit des Menschen und verstößt gegen Art. 1 und 2 Grundgesetz. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil hierzu ausgeführt, dass die Möglichkeit einer ständigen Beobachtung „abweichender Verhaltensweisen“ nicht nur „die individuellen Entfaltungsmöglichkeiten des Einzelnen, sondern auch das Gemeinwohl“ beeinträchtigt. Die von mir eingangs geforderte gesetzliche Regelung ist deshalb dringend notwendig, damit das Entstehen einer solchen flächendeckenden Überwachungsinfrastruktur verhindert wird.

5.6.5 Datenerhebung, -speicherung und -übermittlung von sog. Schulschwänzern

In der Presse war über einen „Sicherheitspakt“ der Stadt Nürnberg mit der örtlichen Polizeidirektion berichtet worden, der auch polizeiliche Maßnahmen gegen sog. Schulschwänzer vorsehe. Diese würden von einem uniformierten Polizisten in die Klasse hineingeführt. Nach dem Presseartikel würden „Schwänzer“ außerdem zumindest für ein Schuljahr gespeichert.

Ich habe dies zum Anlass genommen, das zuständige Polizeipräsidium um Mitteilung zu bitten, ob im dortigen Zuständigkeitsbereich personenbezogene Daten von Kindern, die der Schule unerlaubt fernbleiben, in polizeilichen Dateien, ggf. in welchen und mit welcher Speicherungsdauer erfasst werden. Dabei habe ich auch darauf hingewiesen, dass ich ein Hineinführen von „Schulschwänzern“ durch uniformierte Polizeibeamte bis ins Klassenzimmer für den Zweck der Unterbindung einer betreffenden Ordnungswidrigkeit für nicht erforderlich halte, weil hierfür z. B. eine Übergabe im Sekretariat der Schule ausreichend ist. Rechtlich würde eine solche „Hineinführung“ die Übermittlung personenbezogener Daten des Betroffenen an seine Mitschüler beinhalten, weil diese den beschriebenen Umständen unschwer entnehmen können, dass der betreffende Mitschüler beim „Schwänzen“ von der Polizei aufgegriffen wurde.

Die Polizei hat mitgeteilt, dass der polizeiliche Schriftverkehr mit den zuständigen Stellen der Stadt sowie die polizeilichen Maßnahmen selbst in der polizeilichen Vorgangsverwaltung zum Zwecke der innerdienstlichen Verwaltung der Vorgänge und zur Dokumentation der polizeilichen Maßnahmen gespeichert würden. Eine gesonderte Datei werde nicht geführt. Dabei erfolge eine Speicherung in der Regel nur bis zum Ablauf des jeweiligen Schuljahres. Bei Zuführungen von Minderjährigen zur Schule würden in keinem Fall die betroffenen Schüler durch Polizeibeamte unmittelbar in die Klasse hineingeführt.

Die berichtete Vorgehensweise der Polizei ist datenschutzrechtlich nicht zu beanstanden. Hierzu ist zunächst festzustellen, dass gem. Art. 119 Abs. 1 Nr. 3 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen derjenige, der als Schulpflichtiger am Unterricht oder an den sonstigen verbindlichen Schulveranstaltungen vorsätzlich nicht teilnimmt, eine Ordnungswidrigkeit begeht. Nach § 53 Abs. 1 Satz 1 des Gesetzes über Ordnungswidrigkeiten haben die Behörden und Beamten des Polizeidienstes nach pflichtgemäßem Ermessen Ordnungswidrigkeiten zu

erforschen und dabei alle unaufschiebbaren Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Daraus ergibt sich die grundsätzliche Zuständigkeit der Polizei für Maßnahmen gegen sog. Schulschwänzer.

Nach Art. 38 Abs. 1 Polizeiaufgabengesetz 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 polizeiliche Vorgangsverwaltung dient den Polizeidienststellen zum Nachweis und zum Auffinden des zu einem polizeilich relevanten Ereignis angefallenen Schriftverkehrs für einen angemessenen Zeitraum, der zeitlich befristeten Dokumentation polizeilicher Maßnahmen sowie der Information von Polizeibeamten über die in ihrem Zuständigkeitsbereich angefallenen Ereignisse und ist Grundlage für die Bearbeitung von Beschwerden, Eingaben, Anträgen und Anfragen sowie für die aktuelle und ggf. künftige polizeiliche Sachbearbeitung. Dabei hängt die Zulässigkeit der Speicherung personenbezogener Daten von Kindern und Jugendlichen nicht von der Zustimmung eines gesetzlichen Vertreters ab.

5.6.6 Formblatt Beschuldigtenvernehmung

Das Formblatt Beschuldigtenvernehmung findet in einheitlicher Ausgestaltung bei der gesamten bayerischen Polizei Verwendung. Es dient der Dokumentation der Vernehmung des Beschuldigten. Wird der Beschuldigte nicht polizeilich vernommen, werden seine personenbezogenen Daten in der Regel aus polizeilichen oder polizeilich erschließbaren Informationssystemen entnommen und in das Formblatt eingetragen. Zu Klarstellung wird das Ankreuzfeld „erhobene Personalien“ gekennzeichnet.

Ein Bürger hat sich an mich gewandt, nachdem er über seinen Rechtsanwalt Akteneinsicht bei der Staatsanwaltschaft erlangt hatte. Dabei hatte er festgestellt, dass in dem Formblatt zu seinen „erhobenen Personalien“ unter der Rubrik „Vorstrafen“ der Vermerk „sexueller Missbrauch von Schutzbefohlenen“ eingetragen war. Ich habe die Speicherung des Vermerks „sexueller Missbrauch von Schutzbefohlenen“ als unrichtig und deshalb unzulässig beurteilt, weil das der Speicherung zugrundeliegende Verfahren nicht mit einer gerichtlichen Bestrafung abgeschlossen worden war. Vielmehr war das Verfahren gegen den Betroffenen eingestellt worden. Das Poli-

zeipräsidium teilte mir auf Vorhalt mit, dass unter der Rubrik „Vorstrafen“ seit jeher nicht nur Vorstrafen sondern unter anderem auch eingestellte Verfahren eingetragen werden. Ich habe eine Änderung verlangt, weil die Bezeichnung „Vorstrafen“ die unzutreffende Annahme nahelegt, dass es sich bei den unter dieser Rubrik eingetragenen Ermittlungsverfahren tatsächlich um gerichtliche Vorstrafen handelt. Das Polizeipräsidium hat daraufhin vorgeschlagen, diese Rubrik wie folgt zu formulieren: „Vorstrafen, strafrechtliche Ermittlungsverfahren, Maßregeln der Besserung und Sicherung“. Ich habe das als Kompromiss letztlich akzeptiert, da durch die Änderung wenigstens klargestellt ist, dass es sich bei dem Eintrag nicht um eine Vorstrafe handeln muss. Das Formblatt wird bayerneinheitlich geändert.

5.7 Kontrolle von Datenübermittlungen

5.7.1 Datenübermittlung an das Luftamt Südbayern

In einem Fall hat sich ein Bürger an mich gewandt, weil ihm nach den Ermittlungen des Luftamtes Südbayern im Rahmen der Sicherheitsprüfung der Zugang in den Sicherheitsbereich des Flughafens München verwehrt worden sei. Es sei aber aufgefordert worden, das Luftamt über den Ausgang der von der Polizei mitgeteilten Strafverfahren zu unterrichten. Ich habe dazu festgestellt, dass einzelne Speicherungen bereits aus den Jahren 1980 bis 1984 herrührten. Die jüngste Speicherung war aus dem Jahre 1996. Dazwischen waren keine Erkenntnisse gespeichert. Daraus ergab sich, dass die Speicherungen aus den Jahren 1980 bis 1984 spätestens mit Ablauf der Höchstfrist von 10 Jahren, Ende des Jahres 1994 hätten gelöscht werden müssen. Wie sich weiter herausstellte, waren die Kriminalakten zu den Verfahren aus 1980 bis 1984 bei der aktenführenden Polizeidirektion nicht mehr vorhanden. Die Ursache, weshalb die Speicherungen im Kriminalaktennachweis nicht gelöscht worden waren, konnte letztendlich nicht mehr geklärt werden. Aufgrund der Unzulässigkeit der Speicherungen aus den Jahren 1980 bis 1984 war auch deren Übermittlung an das Luftamt Südbayern rechtswidrig. Dem Luftamt Südbayern habe ich deshalb mitgeteilt, dass diese Speicherungen zum Zeitpunkt ihrer Übermittlung unzulässig gespeichert waren und deshalb von der Polizei gelöscht wurden.

5.7.2 Datenübermittlungen bei Alkoholkontrollen an das Gesundheitsamt

Polizeibeamte hatten einen Bürger während eines Zeitraums von über 2 Jahren vier Mal zum Teil im Zusammenhang mit dem Führen eines Kraftfahrzeugs angetroffen, bei ihm jeweils u.a. Alkoholgeruch festgestellt und daraufhin weitere Maßnahmen gegen ihn ergriffen. Von zwei Ereignissen unterrichtete die zuständige Polizeidienststelle mit Blick auf eine mögliche Alkoholabhängigkeit das örtliche Gesundheitsamt, welches den Betroffenen daraufhin „zur Beratung“ vorlud.

Ich habe die zuständige Polizeidirektion darauf hingewiesen, dass die für eine Datenübermittlung an das Gesundheitsamt notwendigen rechtlichen Voraussetzungen nicht vorgelegen hatten.

Nach Art. 40 Abs. 3 Polizeiaufgabengesetz kann die Polizei von sich aus anderen Behörden oder öffentlichen Stellen, die für die Gefahrenabwehr zuständig sind, die bei ihr vorhandenen personenbezogenen Daten übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint. Nach Art. 11 Abs. 1 Satz 2 Nr. 2 des Gesetzes über den öffentlichen Gesundheitsdienst ist das Gesundheitsamt u.a. zuständig für die gesundheitliche Beratung für Menschen, die an einer Sucht leiden.

Die Polizei führte aus, dass sie eine mögliche Suchtgefährdung des Betroffenen annehmen konnte, weil dieser bei der einen Kontrolle „sehr deutlich“, bei der anderen „sichtlich“ unter Alkoholeinfluss gestanden hätte.

Diesen Umständen habe ich keine ausreichenden Anhaltspunkte für eine Suchtkrankheit oder -gefährdung entnehmen können. Allein die mehrmalige Feststellung, dass der Betroffene Alkohol zu sich genommen hat, rechtfertigt keinesfalls die Annahme einer entsprechenden Abhängigkeit. Soweit beim Betroffenen überhaupt Alkoholmessungen durchgeführt wurden, hatten diese jeweils Atem- oder Blutalkoholwerte ergeben, die noch keinen Ordnungswidrigkeitstatbestand erfüllten. Im Übrigen wurde die Alkoholisierung allein aufgrund des äußeren Erscheinungsbildes (z. B. Alkoholgeruch, unsichere Motorik, schwere Aussprache) beurteilt. Soweit derartige Auffälligkeiten in Verbindung mit geringen Alkoholwerten festgestellt wurden, dürfte dies jedoch eher gegen eine Alkoholgewöhnung sprechen. So sieht das Staatsministerium des Innern Anhaltspunkte für erheblichen oder chronischen Alkoholmissbrauch z. B. gerade in einem relativ unauffälligen Verhalten im Straßenverkehr trotz hohen Blutalkoholgehalts. Zwar mag es zutreffen, dass nicht nur die Höhe der festgestellten Alkoholwerte, sondern auch Zeitdauer und Regelmäßigkeit der Alkoholaufnahme die Abhängigkeit widerspiegeln. Im vorliegenden Fall hatten jedoch die Polizeibeamten in einem relativ langen Zeitraum von mehr als 2 Jahren beim Betroffenen lediglich in vier Fällen Anzeichen für einen gewissen Alkoholkonsum festgestellt. Diese Vorkommnisse allein rechtfertigten m.E. noch nicht einmal die Annahme einer regelmäßigen Alkoholaufnahme, so dass zur Zeitdauer eines solchen regelmäßigen Konsums gar keine Aussagen getroffen werden können. Von einer Suchtbedeutung, die ggf. eine Datenübermittlung an das Gesundheitsamt gerechtfertigt hätte, kann deswegen hier keine Rede sein.

Auf meine Androhung hin, die erfolgte Datenübermittlung förmlich zu beanstanden, hat mir die Polizeidirektion mitgeteilt, dass die Dienststellenleiter angewiesen wurden, eine Meldung zum Gesundheitsamt künftig erst dann durchzuführen, wenn eine entsprechende Suchtgefährdung bzw. Suchtabhängigkeit nachweislich feststellbar ist.

5.7.3 Datenübermittlung an die Presse/Polizeiliche Presseberichte

In meinem letzten Tätigkeitsbericht (Nr. 5.6.2) hatte ich berichtet, dass ich – aus gegebenem Anlass – gegenüber der Polizei auf die grundsätzliche Problematik bei der Übermittlung personenbezogener Daten durch die Polizei an die Medien eingegangen bin.

Im Zuge meiner routinemäßigen Überprüfung von Presseerklärungen der Polizei bin ich wiederum auf einen polizeilichen Bericht gestoßen, der eine ausreichende Güter- und Interessenabwägung nicht erkennen lässt. Berichtet wird über einen versuchten Einbruch unter Angabe des Alters, des Berufs, des vollständigen und seltenen Vornamens sowie des Anfangsbuchstabens des Nachnamens des Tatverdächtigen.

Ich habe die Polizei darauf hingewiesen, dass der Betroffene durch die Gesamtheit derartiger Individualisierungsmerkmale für sein soziales Umfeld eindeutig kenntlich gemacht wird. Im konkreten Fall war festzustellen, dass die Gefahr der Identifizierung des Betroffenen gerade wegen seines ausgefallenen Vornamens besonders groß war. Der Informationsgehalt für die allgemeine Öffentlichkeit wäre nicht beeinträchtigt worden, wenn auch der Vorname lediglich gekürzt auf den Anfangsbuchstaben genannt worden wäre. Zwar kann grundsätzlich die Angabe des Berufs im Einzelfall dann gerechtfertigt sein, wenn die berufliche Tätigkeit mit der Tatbegehung in einem inneren Zusammenhang steht, im vorliegenden Fall war eine derartige Verbindung jedoch nicht erkennbar. Ich habe die Polizei davon in Kenntnis gesetzt, dass ich diese Datenübermittlung als Verstoß gegen die datenschutzrechtliche Vorschrift des Art. 41 Polizeiaufgabengesetz betrachte und erwäge, in vergleichbaren zukünftigen Fällen eine Beanstandung auszusprechen.

5.8 Kontrolle der Auskunftserteilung über Speicherungen in Dateien

5.8.1 Voraussetzungen und Umfang der Auskunftserteilung

Viele Bürger haben sich wieder an mich gewandt, weil sie bei der Inanspruchnahme Ihres Auskunftsrechts nach Art. 48 Polizeiaufgabengesetz (PAG) von der Polizei aus ihrer Sicht eine unbefriedigende Antwort erhalten hatten. Bei meiner Überprüfung dieser Fälle sowie bei anlassunabhängigen Kontrollen habe ich wieder Mängel bei der Behandlung von Auskunftsersuchen durch die Polizei festgestellt.

Die Frage, unter welchen Voraussetzungen und in welchem Umfang die Polizei Auskunft zu erteilen hat, scheint dabei weiterhin ein nicht gelöstes Problem zu sein. In meinem 18. Tätigkeitsbericht (vgl. Nrn. 5.8.1 und 5.8.2) hatte ich bereits dargestellt, dass bei pauschal formulierten Auskunftsanträgen (z. B. ... möchte ich Auskunft darüber, was über mich bei der Polizei gespeichert wird ...) die Polizei nach den Richtlinien über die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien) grundsätzlich Auskunft über Speicherungen im Kriminalaktennachweis und in der Datei PSV (Vorgangsverwaltungsdateien) zu erteilen hat.

Ein Bürger hat sich an mich gewandt, weil ihm die für die Auskunft zuständige Polizeidirektion trotz eines entsprechenden Antrags die zu seiner Person bestehenden Speicherungen nicht mitgeteilt hatte. Begründet wurde die Auskunftsablehnung mit „zu unpräzisen Angaben“ des Betroffenen über die von ihm angenommenen Speicherungen. Diese Begründung rechtfertigt die Ablehnung der Auskunft nicht. Der Antragsteller soll zwar seinen Antrag präzisieren, um die Auskunft nicht unnötig zu erschweren. Die Auskunftserteilung darf aber nicht allein deshalb verweigert werden, weil der Antrag diesem formalen Erfordernissen nicht entspricht. Der betroffene Bürger hat aufgrund meines Einschreitens Auskunft von der Polizei erhalten.

Ein Polizeipräsidium vertrat trotz der eindeutigen Rechtslage die Auffassung, dass eine Auskunft über den in Vorgangsverwaltungsdateien gespeicherten internen Schriftverkehr nicht zu erteilen sei. Eine solche Begrenzung des Auskunftsanspruchs kennt das Polizeiaufgabengesetz nicht. Der Betroffene hat grundsätzlich uneingeschränkten Anspruch auf Auskunft, auch über die Speicherung seiner personenbezogenen Daten im Zusammenhang mit polizeilichem Schriftverkehr. Nur

bei Vorliegen der abschließend im Gesetz aufgezählten Versagungsgründe kann die Auskunft ganz oder teilweise unterbleiben. Auf die Tatsache der teilweisen oder vollständigen Auskunftsablehnung ist der Betroffene hinzuweisen. Insbesondere darf bei dem Anfragenden nicht der unzutreffende Eindruck erweckt werden, er habe eine Vollauskunft erhalten, obwohl es sich nur um eine Teilauskunft handelt. Das Polizeipräsidium hat sich wegen seiner Auffassung, ob interner Schriftverkehr dem Auskunftsanspruch unterliegt, an das Staatsministerium des Innern gewandt. Eine Antwort des Staatsministerium des Innern liegt mir noch nicht vor.

Bei meiner Prüfung der Behandlung von Auskunftsanträgen bei einem Polizeipräsidium habe ich festgestellt, dass wegen Zuständigkeitsfragen Lücken beim Auskunftsumfang entstehen können. Richtet sich der Auskunftsantrag an die örtliche Polizeidienststelle (in der Regel das Polizeipräsidium oder die Polizeidirektion), wird dieser ohne weitere Veranlassung gegenüber dem Bürger an das Landeskriminalamt (BLKA) abgegeben, soweit auch Speicherungen im Kriminalaktennachweis anderer Polizeipräsidien vorliegen. Das BLKA seinerseits berücksichtigt bei der Auskunftserteilung Speicherungen in den Vorgangsverwaltungsdateien der Polizeipräsidien grundsätzlich nicht. Der Antragsteller wird insoweit wieder an die Präsidien verwiesen, bei denen er seinen Auskunftsantrag gestellt hatte. Durch dieses Verfahren - wenn es vom Betroffenen überhaupt durchschaut wird - verzögert sich eine vollständige Auskunft unverhältnismäßig. Darüber hinaus besteht aber die Gefahr, dass er den Eindruck gewinnt, neben den Speicherungen im Kriminalaktennachweis seien keine weiteren polizeilichen Speicherungen zu seiner Person vorhanden. Ich habe das BLKA und das betreffende Polizeipräsidium aufgefordert, eine praktikable Lösung zu finden, die dem Auskunftsanspruchs des Bürgers gerecht wird. Ein Ergebnis liegt noch nicht vor.

Anlässlich zweier Bürgereingaben habe ich festgestellt, dass dem Antragsteller von der Polizei lediglich die Anzahl seiner Speicherungen mitgeteilt wurde. Diese Form der Mitteilung ist unzureichend. Ohne Kenntnis über den Inhalt der Speicherungen ist die Auskunft weitgehend wertlos, da der Bürger seine ggf. berechtigten Ansprüche auf z. B. Löschung oder Berichtigung der Speicherungen mangels Kenntnis des Sachverhalts nicht wahrnehmen kann. Auf meine Intervention hin wurden die Auskünfte vollständig erteilt.

Ein anderer Bürger begehrte auch Auskunft darüber, an welche Stellen seine gespeicherten personenbezogenen Daten übermittelt wurden. Die Polizei hat ihm zunächst mitgeteilt, dass nach dem PAG kein Anspruch auf die Mitteilung über Empfängerstellen bestehe. Diese Auskunft war unrichtig. Der Bayerische Verwaltungsgerichtshof hat bereits in seinem Urteil vom 17.12.1990 entschieden, dass das grundrechtlich geschützte Recht des Bürgers auf informationelle Selbstbestimmung auch das Recht auf Auskunft über die Empfängerstellen umfasst, da ohne deren Kenntnis das allgemeine Auskunftsrecht nicht realisiert werden kann. Eine Auskunftsablehnung kommt z.B. in Betracht, wenn der Hinweis auf die Empfängerstelle polizeiliche Meldewege offenbart und dies mit dem Geheimhaltungsbedürfnis der Polizei unvereinbar wäre. Nach meiner Intervention hat die Polizei die Auskunft erteilt.

5.8.2 Ablehnung der Auskunft bei zahlreichen Speicherungen

In einem Fall hatte sich ein Bürger an mich gewandt, weil sein Antrag auf Auskunft über seine in polizeilichen Informationssystemen gespeicherten personenbezogenen Daten von der Polizei abgelehnt worden war. Als Grund für die Auskunftsablehnung wurde mir zunächst mitgeteilt, dass über den Antragsteller zahlreiche Speicherungen vorhanden seien. Bei einer Auskunftserteilung sei eine Gefährdung der polizeilichen Aufgabenerfüllung zu besorgen, weil der Antragsteller aufgrund der zwölf Einträge kein „unbeschriebenes Blatt“ sei. Ich habe das zuständige Polizeipräsidium darauf hingewiesen, dass eine hohe Anzahl von Speicherungen für sich genommen noch keinen Ausforschungsverdacht begründet. Andere Gründe für die Auskunftsverweigerung wurden mir nicht genannt und waren auch nicht ersichtlich. Das Polizeipräsidium hat daraufhin die verantwortliche Polizeidienststelle veranlasst, dem Antragsteller Auskunft zu erteilen.

5.8.3 Generelle Ablehnung der Auskunft bei Betäubungsmittelhandel

Nach dem Polizeiaufgabengesetz (PAG) unterbleibt die Auskunft u.a., soweit eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei zu besorgen ist. Im Hinblick hierauf wurde vom Staatsministerium des Innern festgelegt, dass **ohne Einzelfallprüfung in allen Fällen** des unbefugten Rauschgifthandels eine Auskunft unter-

bleibt. In meinem letzten Tätigkeitsbericht (Nr. 5.8.4) hatte ich dargestellt, dass ich dieser Auffassung entgegengetreten bin, weil der Bürger ohne entsprechende Kenntnis keine Möglichkeit hat, evtl. bestehende Ansprüche z.B. auf Berichtigung oder Löschung seiner Daten durchzusetzen. Die Verweigerung der Auskunftserteilung stellt einen erheblichen Eingriff in seine Rechte dar, der unter Beachtung des Verhältnismäßigkeitsgrundsatzes auf besondere Ausnahmen nach Beurteilung des Einzelfalls zu beschränken ist. Die **generelle** Ablehnung der Auskunftserteilung widerspricht dem Gesetz. Art und Umfang des unbefugten Rauschgifthandels sind so verschiedenartig, dass nicht in allen Fällen der Auskunftserteilung eine Gefährdung der polizeilichen Aufgabenerfüllung angenommen werden kann. Dies gilt insbesondere dann, wenn die Durchführung des Strafverfahrens dem Betroffenen ohnehin bekannt ist.
Seit meinem letzten Tätigkeitsbericht bin ich erneut mehrfach an das Innenministerium herangetreten, um eine Änderung der polizeilichen Verwaltungsvorschrift dahingehend zu erreichen. Nach mehreren Besprechungen mit Vertretern des Innenministeriums erklärte sich dieses jedoch lediglich bereit, in der Verwaltungsvorschrift vorzusehen, dass bei Delikten des unbefugten Rauschgifthandels grundsätzlich eine Auskunftsverweigerung in Betracht komme, außer wenn eine besonders sorgfältige Prüfung ergäbe, dass durch die Auskunftserteilung eine Gefährdung der polizeilichen Aufgabenerfüllung nicht zu besorgen ist.

Ich habe das Innenministerium darauf hingewiesen, dass auch eine derartige Regelung gegen Art. 48 PAG verstößt. Aus der gesetzlichen Systematik ergibt sich zweifelsfrei ein Regel-/Ausnahme-Verhältnis dergestalt, dass ohne Vorliegen **tatsächlicher Umstände**, die einen der gesetzlich genannten Auskunftsverweigerungsgründe ergeben, die Auskunft stets erteilt werden muss. Die vom Innenministerium vorgeschlagene Formulierung hätte zur Folge, dass die Auskunft lediglich in Fällen erteilt werden könnte, in denen die Prüfung ausnahmsweise positiv ergibt, dass ein Auskunftsverweigerungsgrund nicht vorliegt. Durch diese Fassung der Richtlinien würde die Auskunftserteilung vom Vorliegen besonderer für die Auskunftserteilung sprechender Umstände abhängig gemacht und hierdurch das gesetzliche Verhältnis von Regel und Ausnahme ins Gegenteil verkehrt. In allen Fällen, in denen die Prüfung weder tatsächliche Umstände für noch gegen eine Gefährdung der polizeilichen Aufgabenerfüllung ergibt, würde keine Auskunft erteilt werden. Eine solche Praxis dürfte erhebliche Auswirkungen haben, weil es in den allermeisten Fällen an solchen tatsächlichen Umstände fehlen wird. Die vom Innenministerium vor-

gesehene Änderung der Richtlinien würde daher an der generellen Auskunftsverweigerung kaum etwas ändern.

Hierauf habe ich in einer persönlichen Besprechung den Staatsminister des Innern hingewiesen. Als Kompromiß habe ich eine Formulierung vorgeschlagen, wonach bei Delikten des unbefugten Rauschgifthandels bezüglich der Nachweise von Kriminal- und Vorgangsakten (KAN und PSV) besonders sorgfältig zu prüfen ist, ob im Einzelfall Versagungsgründe i.S.d. Art. 48 Abs. 2 PAG vorliegen. Ist dies der Fall, sei die Auskunft abzulehnen.

Die Prüfung meines Vorschlags wurde mir zunächst bis Ende Februar 2000 zugesagt. Nach Auskunft des Innenministeriums wird er zur Zeit von einer Arbeitsgruppe verschiedener Polizeipräsidien und des Bayerischen Landeskriminalamts „einer eingehenden Prüfung“ unterzogen. Ein Ergebnis liegt mir trotz eines Diskussionszeitraums von mehr als einem Jahr immer noch nicht vor.

5.8.4 Ablehnung der Auskunft bei laufenden Ermittlungsverfahren

Auf den Auskunftsantrag eines Bürgers über seine bei der Polizei gespeicherten Daten hatte das Bayerische Landeskriminalamt (BLKA) lediglich mit einer Teilauskunft geantwortet. Wegen der Speicherung eines Tatvorwurfs in einem anhängigen Ermittlungsverfahren im Kriminalaktennachweis wurde er an die zuständige Staatsanwaltschaft verwiesen.

Für diese Verweisung sehe ich keine rechtliche Grundlage. Auf meine entsprechende Anfrage teilte das BLKA mit, dass der Anwendungsbereich des Art. 48 Polizeiaufgabengesetz (PAG) nicht die Daten eines noch anhängigen Strafverfahrens umfasse, auch wenn diese Daten in polizeilichen Dateien gespeichert würden, da hierfür allein die Regelungen des Strafverfahrensrechts maßgebend seien.

Diese Auffassung ist unzutreffend. Speichernde Stelle für die präventive Speicherung personenbezogener Daten aus strafrechtlichen Ermittlungsverfahren im Kriminalaktennachweis ist die Polizei. Diese trägt damit die datenschutzrechtliche Verantwortung und die daraus folgenden gesetzlichen Verpflichtungen. Hierzu gehört auch die grundsätzliche Pflicht zur Auskunftserteilung nach Art. 48 PAG („die **Polizei** erteilt..... Auskunft“) bzw. zur Entscheidung über das Vorliegen von gesetzlichen Auskunftsverweigerungsgründen. Diese Entscheidung, die von der Polizei und nicht von der Staatsanwaltschaft zu treffen ist, kann nicht durch eine Verweisung an die Staatsanwaltschaft umgangen werden.

Eine solche Verweisung greift unzulässig in das Recht des Betroffenen auf informationelle Selbstbestimmung ein. Im Einzelfall können Ermittlungsverfahren auch nach mehreren Jahren noch nicht abgeschlossen sein. Ein Aufschieben der gesetzlichen Verpflichtung der Polizei aus Art. 48 PAG für diese Zeit sieht das Gesetz aber nicht vor.

Die vom Innenministerium befürchtete „Aushebelung“ der Entscheidungsbefugnis der Staatsanwaltschaft über die Auskunftserteilung aus einem laufenden Ermittlungsverfahren wegen der Existenz teilweise paralleler Datensammlungen zur Strafverfolgung und zur Gefahrenabwehr sehe ich nicht. Diese kann durch eine Abstimmung zwischen Polizei und Staatsanwaltschaft vermieden werden. Eine solche Abstimmung stellt jedoch einen rein internen Vorgang dar, der

keine Auswirkungen auf die Entscheidungsverpflichtung der Polizei gegenüber dem Betroffenen hat. Verweigert die Staatsanwaltschaft ihr Einvernehmen mit einer Auskunftserteilung an den Betroffenen, weil hierdurch Zwecke des Strafverfahrens gefährdet würden, kann grundsätzlich ein Auskunftsverweigerungsgrund gem. Art. 48 Abs. 2 PAG angenommen werden, so dass eine Auskunftserteilung unterbleibt.

Ich habe nach ergebnisloser Diskussion mit dem BLKA und dem Innenministerium darauf hingewiesen, dass ich den dem bisherigen Verfahren zugrundeliegenden Verstoß gegen Art. 48 PAG beanstanden werde, wenn eine Änderung des Verfahrens weiter abgelehnt wird. Das Innenministerium wird sich nunmehr mit dem ebenfalls betroffenen Justizministerium abstimmen und anschließend wieder auf mich zukommen. Die Äußerung des Innenministeriums steht noch aus.

5.9 Abfragen polizeilicher Informationssysteme

In meinem 18. Tätigkeitsbericht (vgl. Nr. 5.7) hatte ich insbesondere die Problematik nicht dienstlich veranlasster Abfragen in polizeilichen Informationssystemen aber auch von dienstlichen Abfragen im sozialen Umfeld von Polizeibediensteten dargestellt. Wegen dieser Problematik habe ich gefordert, dass dienstlich veranlasste Dateiabfragen im sozialen Umfeld des Polizeibediensteten bzw. in eigener Sache grundsätzlich nicht von diesem selbst, sondern - nach Unterrichtung des Vorgesetzten - von einem unbeteiligten Polizeibeamten durchgeführt werden sollten. Das Staatsministerium des Innern hat mir zugesichert, die landesweite Anordnung eines solchen Verfahrens zu prüfen, nachdem es die Erfahrungen eines Polizeipräsidiums - welches die Unterrichtung des Vorgesetzten vorsieht - ausgewertet hat. Nach nunmehr fast zwei Jahren hat mir das Staatsministerium des Innern - ohne auf die Erfahrungen des Pilotprojekts einzugehen - mitgeteilt, dass es eine generelle landesweite Anordnung des Verfahrens wegen der Fülle (nicht genannter) anderer Vorschriften und Richtlinien, in denen die gleiche Materie behandelt werde, nicht für angezeigt halte. Überdies verweist das Innenministerium auf bereits realisierte und geplante Maßnahmen im Aus- und Fortbildungsbereich, im Bereich der Dienstaufsicht und auf technische Maßnahmen.

Die Reaktion des Innenministeriums ist mir völlig unverständlich. Offenbar ist die von mir geforderte und von einem Polizeipräsidium teilweise bereits praktizierte Verfahrensweise zur Vermeidung von Abfragen bei eigener Betroffenheit nicht gewünscht. Weder sind mir polizeiliche Vorschriften bekannt, die diese Materie regeln, noch haben Ausbildungs- und Fortbildungsinhalte zur Grundsatzproblematik bei Rechtseingriffen und zum Datenschutz eine einer konkreten schriftlichen Anordnung vergleichbare Wirkung. Der Hinweis auf die in Bayern praktizierte 100-Prozent-Protokollierung und die anlassunabhängige Zusatzprotokollierung polizeilicher Abfragen geht in diesem Zusammenhang fehl, da diese Protokollierungen nur unzulässige Abfragen verhüten bzw. offenlegen können. Die Unzulässigkeit von Abfragen bei eigener Betroffenheit will das Innenministerium aber gerade nicht feststellen: „Insbesondere aus praktischen Überlegungen heraus sollte vermieden werden, dass der einzelne Polizeibeamte zur Erlangung einer für seine Aufgabenerfüllung wichtigen Information langwierige und komplizierte Abfrageprozeduren überwinden muss, die letztlich negative Auswirkungen auf Motivation und Akzeptanz haben“. Andererseits wird eingeräumt, dass das Pilotverfahren wegen der sich im Bereich des Poli-

zeipräsidiums häufenden Verstöße gegen Datenschutzbestimmungen zur Verbesserung der Datensicherheit erforderlich war.

Ich werde das Innenministerium nochmals auffordern anzuordnen, die datenschutzrechtlich problematischen Abfragen selbst betroffener Polizeibeamter zu unterlassen, da in diesem Bereich die Gefahr besonders groß ist, die Grenzen zwischen dienstlich veranlasster und missbräuchlicher oder strafrechtlich relevanter Nutzung zu überschreiten. Den praktischen Überlegungen des Innenministeriums kommt angesichts dieser Gefahr und der vergleichsweise wohl geringen Zahl der kritischen Abfragen keine wesentliche Bedeutung zu.

In künftigen Fällen werde ich eine Beanstandung prüfen.

5.10 Beteiligung des Datenschutzbeauftragten durch das Innenministerium im Polizeibereich

Bereits oben unter Nr. 5.5 habe ich dargelegt, dass nach § 34 Abs. 2 Bundeskriminalamtgesetz (BKAG) die Errichtungsanordnung für eine beim Bundeskriminalamt (BKA) geführte automatisierte Datei des polizeilichen Informationssystems (Verbunddateien) auch der Zustimmung der zuständigen Innenministerien und Senatsinnenverwaltungen der Länder bedarf. Meine Information durch das Staatsministerium des Innern im Rahmen von Zustimmungsverfahren nach § 34 Abs. 2 BKAG war in der Vergangenheit jedoch nicht stets im erforderlichen Umfang gewährleistet:

- So teilte mir das Innenministerium zu der Errichtungsanordnung für die DNA-Analyse-Datei erst mit Schreiben vom 17.04.1998 mit, dass dem Entwurf vom 14.04.1998 bereits zugestimmt worden sei. Ein Entwurfstext war mir jedoch nicht übermittelt worden.

- Bereits in einem Schreiben vom 09.06.1999 äußerte sich ein anderer Datenschutzbeauftragter zu dem ihm vorliegenden Entwurf einer Errichtungsanordnung (Stand 04.02.1999) für die Verbunddatei ViCLAS. Mir wurde vom Innenministerium ein Entwurf für die Verbunddatei erst am 31.03.2000, kurz vor dem Abschluss des Zustimmungsverfahrens übersandt.

- Der Entwurf einer Errichtungsanordnung über die Verbunddatei „Arbeitsdatei PIOS-Rauschgift“ wurde mir erst mit Schreiben vom 29.03.2000 zugeleitet, obwohl ein anderer Datenschutzbeauftragter bereits am 07.02.2000 in der Lage gewesen war, eine Stellungnahme zum überarbeiteten Entwurf einer Errichtungsanordnung abzugeben.

In zwei anderen Fällen wurde ich über datenschutzrechtlich bedeutsame Regelungen überhaupt nicht in Kenntnis gesetzt:

- Erst im Januar 1998 habe ich von einem Schreiben des Innenministeriums vom 23.07.1996 erfahren, in welchem gegenüber der polizeilichen Praxis eine einheitliche und meines Erachtens gesetzeswidrige Auslegung der polizeirechtlichen Befugnis für Speicherungen im Kriminalaktennachweis (Art. 38 Abs. 2 Polizeiaufgabengesetz, PAG) verbindlich vorgege-

ben wurde. In diesem Schreiben wurde insbesondere festgelegt, dass die in Art. 38 Abs. 2 Satz 4 PAG angesprochenen Fälle von geringerer Bedeutung in der von der Verwaltung hierzu erlassenen Ausführungsvorschrift **abschließend** aufgezählt seien (vgl. Nr. 5.3.1.4).

- Erst anlässlich meiner datenschutzrechlichen Prüfung bei einer Polizeidirektion am 01./02.03.2000 wurde mir ein Schreiben des Innenministeriums vom 18.01.2000 sowie ein hierauf bezogenes Fernschreiben des Bayerischen Landeskriminalamts (BLKA) vom 01.02.2000 zur Kenntnis gebracht. Danach könne für Speicherungen in der DNA-Analyse-Datei im Rahmen der Retrograderfassung von Verurteilten einer Straftat von erheblicher Bedeutung als für den Beginn der Speicherungsfrist maßgebliches Ereignis stets das Datum des richterlichen Beschlusses oder, in Fällen der Freiwilligkeit, der Zeitpunkt der Freiwilligkeitserklärung angesehen werden. Bei der Speicherung im Kriminalaktennachweis sei dies analog anzuwenden. In einem weiteren Schreiben stellt das BLKA hierzu ergänzend fest, dass die Festlegung der Aussonderungsprüffrist in der DNA-Analyse-Datei, die auch die Eingabe einer Speicherungsfrist von **mehr als zehn Jahren** erlaube, grundsätzlich an die des Kriminalaktennachweises gebunden sei, in dem bei bestimmten Sexualdelikten Aussonderungsprüffristen von 20 Jahren vergeben worden seien. Die Problematik habe ich oben unter Nr. 5.5.2 eingehend dargestellt.

Ich habe mich an den Amtschef des Innenministeriums gewandt und gebeten, darauf hinzuwirken, dass ich künftig in datenschutzrechtlich bedeutsamen Angelegenheiten zum Zwecke der Erfüllung der mir gesetzlich zugewiesenen Aufgaben rechtzeitig beteiligt werde. Zur Begründung habe ich ausgeführt, dass die in Art. 32 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz festgelegte Pflicht aller öffentlichen Stellen, den Landesbeauftragten für den Datenschutz in der Erfüllung seiner Aufgaben zu unterstützen, u.a. beinhaltet, dass ich von der Verwaltung rechtzeitig über Planungen zu Regelungen datenschutzrechtlich relevanter Angelegenheiten oder deren Umsetzung unterrichtet werde.

Der Amtschef des Innenministeriums hat in seiner Antwort ausgeführt, dass seine Behörde stets das Ziel im Auge habe, mich über Planungen bedeutender Informationsvorhaben rechtzeitig zu unterrichten. Soweit es im einen oder anderen Fall vorgekommen sein sollte, dass eine Unter-

richtung meiner Behörde unterblieben ist, werde dies bedauert. Die Ursache hierfür sei jedoch ausschließlich auf Büroversehen zurückzuführen.

Ich erwarte, dass die gesetzliche Pflicht, mich (rechtzeitig) über datenschutzrechtlich bedeutsame Regelungen zu informieren, vom Innenministerium und seinen nachgeordneten Behörden in Zukunft eingehalten wird.
Über die vom Polizeipräsidium München als Reaktion auf interne Probleme geplante Arbeitsdatei zur Früherkennung von Fehlentwicklungen im personellen Bereich war ich zwar vom Innenministerium rechtzeitig informiert worden. Wegen der vorgesehenen namentlichen Speicherung auch beschwerdeführender Bürger hatte ich Bedenken erhoben und das Innenministerium gebeten, ggf. für die Speicherung sprechende Gründe darzulegen. Statt einer Antwort in der Sache hat das Innenministerium lediglich mitgeteilt, dass es die nach dem Gesetz erforderliche datenschutzrechtliche Freigabe für den Einsatz der Arbeitsdatei erteilt habe. Eine solche Beteiligung erfüllt ihren Sinn nicht und wird der Unterstützungsverpflichtung des Innenministeriums nach dem Bayerischen Datenschutzgesetz nicht gerecht. Ich erwarte eine Stellungnahme zur angesprochenen datenschutzrechtlichen Problematik. Darauf habe ich das Innenministerium hingewiesen. Eine Antwort des Innenministeriums steht noch aus.

5.11 Europol

In meinem letzten Tätigkeitsbericht (Nr. 5.9.2) hatte ich mitgeteilt, dass das Europäische Polizeiamt (Europol) in Kürze seine Tätigkeit auf der Grundlage des Europol-Übereinkommens aufnehmen werde. Mittlerweile sind sämtliche Durchführungs- und Ausführungsbestimmungen zur Konvention, von deren In-Kraft-Treten die Tätigkeitsaufnahme von Europol abhing, ratifiziert worden. Dies gilt etwa für die Geschäftsordnung des Beschwerdeausschusses sowie die Ausführungsbestimmungen über Verbindungen von Europol mit Drittstaaten und –stellen und den Umgang mit den wechselseitig übermittelten Daten. Europol hat nunmehr am 01.07.1999 seine Tätigkeit aufgenommen.

Bereits in meinem letzten Tätigkeitsbericht hatte ich über die Durchführungsbestimmungen zu den sog. Arbeitsdateien zu Analysezwecken berichtet. Bei der Arbeit mit diesen Analysedateien liegt gegenwärtig noch der Schwerpunkt der Tätigkeit von Europol. Das zentrale Informationssystem der Behörde ist dagegen bislang aufgrund von technischen Problemen noch nicht arbeitsfähig. Während in diesem Informationssystem nur Daten von Personen gespeichert werden dürfen, die bereits wegen einer Straftat, für die Europol zuständig ist, verurteilt wurden oder zumindest verdächtigt sind oder bei denen bestimmte schwer wiegende Tatsachen die Annahme rechtfertigen, dass sie solche Straftaten begehen werden, erlauben die Vorschriften zu den Analysedateien auch die Speicherung und Verarbeitung der Daten eines weit größeren Personenkreises (z.B. in Betracht kommende Zeugen, mögliche Opfer, Kontakt- und Begleitpersonen). Damit ist der Kreis der möglichen Betroffenen so weit gezogen, dass theoretisch die Daten nahezu jedes Bürgers ohne sein Wissen erfasst und verarbeitet werden können.

Zu Recht wird ferner das Fehlen einer begleitenden Rechtskontrolle der Analysetätigkeit im Zusammenhang mit Ermittlungsverfahren durch eine für Europol zuständige Staatsanwaltschaft gerügt. Auch die bereits in meinem letzten Tätigkeitsbericht geäußerte Kritik an den eingeschränkten Rechtsschutzmöglichkeiten für den Bürger behält weiterhin ihre Berechtigung.

Auf der Grundlage der Bestimmungen über den Datenaustausch zwischen Europol und Drittstaaten und -stellen werden zur Zeit Verhandlungen mit Interpol und mit Norwegen geführt. Im Rahmen dieser Verhandlungen wird auch geprüft, ob die Verhandlungspartner über ein für

die ins Auge gefassten Datenübermittlungen ausreichendes Datenschutzniveau verfügen. Für die nahe Zukunft sind Verhandlungen mit Polen, Ungarn und Island geplant.
Neben rechtlichen Problemen im Zusammenhang mit den wechselseitigen Datenübermittlungen mit Drittstaaten und -stellen besteht auch der grundsätzliche Mangel einer direkten parlamentarischen Kontrolle der Behörde Europol fort.

6 Verfassungsschutz

6.1 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Bereich des Verfassungsschutzes waren neben einer Schwerpunktprüfung:

- allgemeine Kontrolle von Speicherungen in Dateien, Karteien und Akten,
- Überprüfung von Errichtungsanordnungen und internen Arbeitsanweisungen
- Kontrolle von Datenerhebungen
- Bürgereingaben

6.2 Ergebnis meiner Prüfungen und Bewertung von Grundsatzthemen

Wie in jedem Berichtszeitraum habe ich auch diesmal wieder mehrtägige Prüfungen beim Landesamt für Verfassungsschutz vorgenommen, war an der Erstellung von Arbeitsanweisungen und Errichtungsanordnungen beteiligt und habe aufgrund von Eingaben datenschutzrechtliche Prüfungen von Einzelfällen vorgenommen. Aufgrund einer über mehrere Wochen andauernden Schwerpunktprüfung, auf die ich noch näher eingehen werde, habe ich einen weiten Überblick über die Speicherungspraxis des Landesamtes für Verfassungsschutz erhalten. Ich konnte dabei und bei den anderen Prüfungen feststellen, dass das Landesamt die datenschutzrechtlichen Bestimmungen grundsätzlich beachtet. Einen großen Teil meiner Feststellungen, meiner Forderungen und der Ergebnisse kann ich im Tätigkeitsbericht nicht darstellen, da diese dem Geheimschutz unterliegen, an den auch ich gebunden bin. Einzelne Feststellungen habe ich im Folgenden dargestellt.

6.2.1 Angebliche Speicherung von Dossiers über demokratische Politiker und Prominente

In einigen Medienberichten wurde der Vorwurf erhoben, das Bayerische Landesamt für Verfassungsschutz (LfV) habe rechtswidrig „Dossiers“ über deutsche demokratische Politiker und Prominente angelegt. Ich habe dies zum Anlass genommen, diesen Vorwürfen im Rahmen einer umfangreichen Überprüfung beim LfV nachzugehen, um die mich auch der Staatsminister des Innern gebeten hatte.

Die Prüfung hat erhebliche Arbeitskapazitäten in Anspruch genommen. Sie wurde über ca. 5 Wochen an insgesamt 14 Tagen von mehreren Mitarbeitern im Landesamt durchgeführt. Dabei wurde der Datenbestand des Amtes untersucht und dabei die den Dateien zugrunde liegenden Aktenbestände (einschließlich der Geheimunterlagen) herangezogen. Die Prüfung umfasste in Bezug auf das Informationssystem IBA den Zeitraum von 1993 (seitdem besteht das System) bis zum Abschluss der Prüfung, sowie die in dieses System übernommenen Informationen aus dem Vorläufersystem auf insgesamt 86 Protokolldatenbändern. In Bezug auf das Registratur-Aktenverwaltungssystem wurde der gesamte Datenbestand erfasst, in Bezug auf die Personen- und Sachakten der gesamte von uns als relevant angesehene Bestand (ca. 250 Aktenordner und Dokumente).

Personenakten im Sinne der Vorwürfe habe ich nicht festgestellt. Soweit nichtextremistische Politiker in nicht suchfähig abgelegten Aktenstücken erwähnt werden, handelte es sich zumeist um Hinweise auf Veranstaltungen oder Medien extremistischer Organisationen, in denen diese Politiker Erwähnung fanden. Dies ist zulässig.

Die außerordentlich tief gehende Prüfung hat aber zwei Kritikpunkte außerhalb des eigentlichen Prüfthemas erbracht. Zum einen habe ich unzulässige Hinweise auf das Intimleben von Personen im Bericht eines Informanten festgestellt. Das LfV hat auf meine Anregung hin die entsprechenden Passagen unkenntlich gemacht. Es hat mir zudem versichert, das Intimleben betreffende Informationen nicht mehr zu speichern, soweit diese nicht für die Aufgabenerfüllung des Amtes zwingend notwendig sind. Zum anderen war die Aufbewahrungsfrist einer Personenakte bereits abgelaufen, die deswegen dem Archiv hätte angeboten oder ausgesondert werden müssen. Das LfV war zu letztem Punkt davon ausgegangen, dass entsprechend der Archivvereinbarung das

Angebot erst nach 30 Jahren notwendig sei. Diese Vereinbarung kann jedoch die gesetzlichen Bestimmungen über die Speicherung nicht ändern (vgl. im einzelnen Nr. 6.2.4).
Das Ergebnis meiner Prüfung habe ich im Detail dem parlamentarischen Kontrollgremium des Bayerischen Landtags vorgetragen und meinen Prüfbericht dem Staatsministers des Innern zugeleitet.

6.2.2 Speicherungsfristen in Fachdateien

Im Rahmen meiner anlassunabhängigen regelmäßigen Prüfung beim Landesamt für Verfassungsschutz bin ich wiederum auf einen Fehler gestoßen, der bereits in der Vergangenheit immer wieder Anlass zu Kritik gegeben hatte.

Der Beginn des Laufs einer Speicherungsfrist in den elektronischen Fachdateien des Landesamtes für Verfassungsschutz, IBA und NADIS, richtet sich nach dem sog. materiellen Erkenntnisdatum. Hierbei handelt es sich um ein im Rahmen der Aufgabenerfüllung des Amtes relevantes Ereignis zu einer Person. Maßgeblich für den Fristbeginn ist der Zeitpunkt des Ereignisses.

In mehreren Fällen habe ich festgestellt, dass nicht der Zeitpunkt des Ereignisses, sondern der Zeitpunkt der Erlangung der Erkenntnis über das Ereignis als Beginn der Speicherungsfrist festgelegt wurde. Dies kann die Speicherungsdauer um Jahre verlängern und ist deshalb nach der geltenden Arbeitsanweisung für die Speicherung und Löschung personenbezogener Daten unzulässig. Ich habe das Landesamt für Verfassungsschutz auf diesen Fehler erneut hingewiesen. Es hat mir versichert, ihn durch entsprechende Aufklärung seiner Mitarbeiter abzustellen. Speicherungen, die bei Zugrundlegung des zutreffenden Erkenntnisdatums schon zu löschen gewesen wären, wurden unverzüglich aus den Dateien gelöscht.

6.2.3 Speicherung im Zusammenhang mit Scientology-Organisation und Übermittlung von Daten über die Mitgliedschaft bei Scientology-Organisation an öffentliche Arbeitgeber

Wie ich in meinem 18. Tätigkeitsbericht (vgl. Nr. 6.2.2) bereits angekündigt hatte, habe ich eine Prüfung von Datenspeicherungen im Zusammenhang mit der Scientology-Organisation beim Landesamt für Verfassungsschutz vorgenommen. Dabei habe ich keine unzulässigen Speicherungen feststellen können.

Es wurde die Frage an mich herangetragen, ob personenbezogene Daten im Zusammenhang mit der Mitgliedschaft bei Scientology vom Landesamt für Verfassungsschutz an öffentliche Arbeitgeber übermittelt werden dürfen. Diese Anfrage habe ich wie folgt beantwortet:

Gemäß Art. 14 Abs. 1 Bayerisches Verfassungsschutzgesetz (BayVSG) darf das Landesamt für Verfassungsschutz personenbezogene Daten an öffentliche Stellen übermitteln, wenn diese die Daten zum Schutz der freiheitlich demokratischen Grundordnung benötigen. Die Innenministerkonferenz hatte auf ihrer Sitzung vom 05./06.06.1997 festgestellt, dass tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen der Scientology-Organisation vorliegen (vgl. 18. Tätigkeitsbericht, Nr. 6.2.2). In einer Bekanntmachung des Staatsministeriums des Innern wurde die Scientology-Organisation deshalb unter der Rubrik „Extremismus anderer Art“ in das Verzeichnis der wichtigsten extremistischen und extremistisch beeinflussten Organisationen aufgenommen. Ausgehend von dieser fachlichen Einschätzung der Innenministerkonferenz halte ich es für zulässig, dass das Landesamt für Verfassungsschutz personenbezogene Daten, soweit sie zur Prüfung der Gewähr der Verfassungstreue von Arbeitnehmern im öffentlichen Dienst erforderlich sind, an den jeweiligen Dienstherrn übermittelt. Dieser muss die Möglichkeit haben, die Erforderlichkeit von Maßnahmen zum Schutz der freiheitlichen demokratischen Grundordnung zu prüfen und diese ggf. auch zu treffen.

6.2.4 Speicherung von Archivakten

Im Rahmen einer anlassunabhängigen Prüfung von Speicherungen des Landesamtes für Verfassungsschutz in der Fachdatei IBA habe ich festgestellt, dass in einem abgeschlossenen Raum des Landesamtes Personen- und Sachakten gelagert werden, die dem Staatsarchiv zur Übernahme hätten angeboten oder vernichtet werden müssen, da die Speicherungsfrist bereits abgelaufen war. Die automatisierten Speicherungen dazu waren zwar in der Datei IBA vorschriftsmäßig gelöscht, die Akten aber nicht vernichtet worden. Das LfV hat zur Begründung auf eine Vereinbarung mit dem Staatsarchiv vorwiesen, wonach Akten des Verfassungsschutzes, 30 Jahre nachdem sie angelegt wurden, dem Staatsarchiv vorzulegen sind. Die Akte entstehe mit dem zeitlich jüngsten Schriftstück.

Dieser Aktenbehandlung habe ich widersprochen. Die Dauer der Aktenaufbewahrung beim Landesamt ist nach den gesetzlichen Bestimmungen und nicht nach Verwaltungsvereinbarungen zu beurteilen. Nach Art. 6 Abs. 1 Bayerisches Archivgesetz haben alle Behörden des Freistaates Bayern dem zuständigen staatlichen Archiv die Unterlagen zur Übernahme anzubieten, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen. Dies ist in der Regel 30 Jahre nach Entstehung der Unterlagen anzunehmen. Für die Dauer der Aktenaufbewahrung beim LfV bestehen aber bereichsspezifische Regelungen. Die Akten sind spätestens dann anzubieten oder zu vernichten, wenn die nach Art. 7 des Bayerischen Verfassungsschutzgesetzes (BayVSG) in Verbindung mit den Arbeitsanweisungen für die Speicherung und Löschung personenbezogener Daten festzusetzenden Speicherungsfristen abgelaufen sind (Art. 8 BayVSG). Bei den im Archivgesetz genannten 30 Jahren handelt es sich um eine Regelfrist im Hinblick auf die zahlreichen unterschiedlichen bayerischen öffentlichen Stellen, die aber neben bereichsspezifischen Regelungen keine Anwendung findet.

Ich habe das LfV deshalb aufgefordert, die Akten, die zur Erfüllung seiner Aufgaben nicht mehr erforderlich sind, unverzüglich dem Staatsarchiv zur Übernahme anzubieten oder, soweit diese nicht übernommen werden, zu vernichten.

Zwischenzeitlich hat das LfV eine entsprechende Vereinbarung mit dem Staatsarchiv getroffen.

6.2.5 Geplante Einführung eines neuen Registratursystems DOMEA

Das Landesamt für Verfassungsschutz (LfV) hat mir seine Absicht mitgeteilt, sein bisheriges Registratursystem REGA (vgl. 18. Tätigkeitsbericht, Nr. 6.2.6) durch ein modernes Dokumentenmangementsystem (DOMEA) abzulösen. Ziel sei es unter anderem, kurzfristig Arbeitsabläufe zu vereinfachen und zu erleichtern, sowie mittel- bis langfristig die Papieraktenhaltung zu reduzieren (elektronische Akte). Zwischenzeitlich hat mir das LfV ein vorläufiges schriftliches Konzept vorgelegt. Aufgrund dieses Konzepts und einer Besprechung des Vorhabens mit dem LfV sehe ich folgende datenschutzrechtliche Schwerpunkte:

- Gemäß Art. 9 Bayerisches Verfassungsschutzgesetz (BayVSG) ist für das Verfahren eine Errichtungsanordnung zu erstellen. Diese ist mir vorzulegen. Obwohl Verfahren, die dem Auffinden von Vorgängen, Anträgen oder Akten dienen (Registraturverfahren) gem. § 2 der Datenschutzverordnung grundsätzlich keiner datenschutzrechtlichen Freigabe nach Art. 26 Bayerisches Datenschutzgesetz und keiner Aufnahme in das Anlagen- und Verfahrensverzeichnis nach Art. 27 Bayerisches Datenschutzgesetzes bedürfen, halte ich eine Errichtungsanordnung für das geplante System für erforderlich, da die vorgesehenen Funktionalitäten des Systems über ein reines Registratursystem hinausgehen. Das LfV hat angekündigt, eine Errichtungsanordnung für DOMEA zu erstellen und mir vorzulegen.

- DOMEA darf außer zum Zweck der reinen Registratur nur unter den Voraussetzungen des Art. 7 Bayerisches Verfassungsschutzgesetz genutzt werden. Für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz nicht relevante Dokumente und Daten müssen deshalb vom Zugriff für den Sachbearbeiter ausgeschlossen sein. Dies soll durch technische und organisatorische Maßnahmen sichergestellt werden.

Eine abschließende datenschutzrechtliche Bewertung bleibt einer eingehenden Prüfung vorbehalten.

6.2.6 Der Auskunftsanspruch nach dem Bayerischen Verfassungsschutzgesetz

Nach Art. 11 Abs. 1 des Bayerischen Verfassungsschutzgesetzes (BayVSG) besteht kein Anspruch auf Auskunft über die beim Landesamt für Verfassungsschutz (LfV) in Dateien oder Akten gespeicherten Informationen. Hat eine Person jedoch ein besonderes Interesse an einer Auskunft über die zu ihr gespeicherten Daten, so entscheidet das Landesamt nach pflichtgemäßem Ermessen über das Auskunftsbegehren (Art. 11 Abs. 1 Satz 2 BayVSG). Nach Art. 11 Abs. 3 BayVSG unterbleibt eine Auskunftserteilung in den dort abschließend aufgeführten Fällen.

Nach Art. 11 Abs. 4 Satz 1 BayVSG bedarf die Ablehnung einer Erteilung von Auskünften keiner Begründung. In seiner Entscheidung vom 11. November 1997 hatte der Bayerische Verfassungsgerichtshof entschieden, dass die Vorschriften des Art. 11 Abs. 1, 3, 4 Satz 1 BayVSG nicht gegen das Grundrecht auf informationelle Selbstbestimmung verstießen. Dies hatte ich in meinem letzten Tätigkeitsbericht (Nr. 6.2.7.1) näher dargestellt.

Von einem besonderen Interesse i.S.d. Art. 11 Abs. 1 Satz 2 BayVSG ist dann auszugehen, 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. Mit Blick darauf, dass diese Vorschrift dem Betroffenen noch keinen Anspruch auf Auskunftserteilung, sondern lediglich auf ermessensfehlerfreie Entscheidung über das Auskunftsbegehren gibt und eine Auskunftserteilung in jedem Fall voraussetzt, dass kein Fall des Art. 11 Abs. 3 BayVSG vorliegt, dürfen die Voraussetzungen für die Annahme eines „besonderen Interesses“ an der Auskunft nicht überspannt werden.

Anlässlich eines konkreten Falles habe ich das LfV darauf hingewiesen, dass eine substanziiert vorgetragene geplante Bewerbung für den öffentlichen Dienst durchaus ein derartiges Interesse an einer Auskunft begründen kann, welches über das bei jedem Bürger gleichermaßen vorhandene Informationsbedürfnis hinausgeht. Ein Bewerber für den öffentlichen Dienst kann z. B. ein Interesse haben, nach vorheriger Auskunftserteilung gegen evtl. – für unzulässig gehaltene – Datenspeicherungen und sich daraus ergebender Sicherheitsbedenken gegenüber dem LfV vorzugehen und mit der Bewerbung einstweilen zu warten.

6.2.7 Datenschutzrechtliche Auswirkungen der Entscheidung des Bundesverfassungsgerichts zur strategischen Fernmeldeüberwachung durch den Bundesnachrichtendienst

In seinem Urteil vom 14.07.1999 zu Abhörmaßnahmen des Bundesnachrichtendienstes hat das Bundesverfassungsgericht Feststellungen getroffen, die für den Schutz von Daten, die durch Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis erhoben werden, und darüber hinaus nach meiner Auffassung, wie der der anderen Datenschutzbeauftragten, für personenbezogene Daten Bedeutung haben, die durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel. Die zentralen Aussagen der Entscheidung hat die 59. Datenschutzkonferenz auf ihrer Sitzung am 14./15.03.2000 in einer Entschließung zusammengefasst und die datenschutzrechtlichen Konsequenzen für Gesetzgeber und Verwaltung dargestellt (siehe hierzu Anlage 15).

Auf die datenschutzrechtlichen Folgerungen des Urteils habe ich den Vorsitzenden der G-10-Kommission des Bayerischen Landtags, das Innenministerium und das Landesamt für Verfassungsschutz hingewiesen. Dabei bin ich insbesondere auch auf die Forderung des Bundesverfassungsgerichts eingegangen, dass auch im Bereich der Landesverwaltung eine ausreichende Kontrolle von Eingriffen in das Fernmeldegeheimnis sichergestellt sein müsse. Die vom Bundesverfassungsgericht aufgestellten Grundsätze beanspruchen nicht nur Geltung für die an die Landesbehörden übermittelten Daten, sondern haben nach meiner Einschätzung auch Bedeutung für Eingriffsmaßnahmen, die von Landesbehörden angeordnet werden, für den gesamten anschließenden Prozess der Verwertung dieser Daten einschließlich deren Übermittlung an andere Behörden, für die Datenlöschung und die Benachrichtigung von Betroffenen. Die Regelung im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 Grundgesetz, G-10-Gesetz), wonach die G-10-Kommission des Bundestages über die Zulässigkeit und Notwendigkeit der Beschränkungsmaßnahmen entscheidet, ist nach dem Urteil des Gerichts mit dem Grundgesetz unvereinbar, da sie nicht hinreichend gewährleistet, dass die Kontrolle den gesamten Prozess der Erfassung und Verwertung der Daten umfasst. Da die entsprechende bayerische Vorschrift in Art. 2 des Bayerischen Ausführungsgesetzes zum G-10-Gesetz inhaltlich

gleich lautet, ist auch insofern eine gesetzliche Klarstellung des Umfangs der Kontrollbefugnis der G-10-Kommission des Bayerischen Landtags erforderlich.

Das Innenministerium hält eine gesetzliche Klarstellung dieser Vorschrift für sinnvoll, will aber zunächst abwarten, bis der Bundesgesetzgeber dem entsprechenden Regelungsauftrag des Bundesverfassungsgerichts zur Änderung des G-10-Gesetzes entsprochen hat.

Aufgrund des Urteils des Bundesverfassungsgerichts sind aber meines Erachtens noch folgende Änderungen bayerischer Gesetze veranlasst:

- Das Bundesverfassungsgericht hat festgestellt, dass sich die Zweckbindung nur gewährleisten lässt, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Von Verfassungs wegen sei daher eine entsprechende Kennzeichnung geboten. Im Zusammenhang mit o. e. Eingriffsmaßnahmen fehlen gesetzliche Vorschriften zur Kennzeichnung der betreffenden Daten jedoch völlig. Im Bereich des bayerischen Landesrechts sind insofern die Regelungen zum sog. Lauschangriff in Art. 34 Polizeiaufgabengesetz (PAG) und Art. 6 Abs. 4 und 5 Bayerisches Verfassungsschutzgesetz (BayVSG) entsprechend zu ergänzen.

- Das Bundesverfassungsgericht hat ferner festgestellt, dass die Übermittlung der betreffenden Daten zu protokollieren sei, um eine hinreichende Kontrolle der Übermittlung zu ermöglichen. Insofern sieht das Landesrecht lediglich in Art. 14 Abs. 4 Satz 2 BayVSG vor, die Datenübermittlung durch das Landesamt für Verfassungsschutz an Private aktenkundig zu machen.

  Im Übrigen entsprechen die vorhandenen Übermittlungsvorschriften im BayVSG und im PAG schon aufgrund des Fehlens entsprechender Protokollierungspflichten nicht den Vorgaben des Bundesverfassungsgerichts.

- Schließlich wurde festgestellt, dass die Vernichtung und Löschung derartiger Daten zu protokollieren sei. Im Bereich des bayerischen Rechts fehlt eine derartige Vorschrift für Daten

aus Maßnahmen des verdeckten Einsatzes technischer Mittel in oder aus Wohnungen gem. Art. 34 PAG.

In diesem Sinne habe ich mich erneut an das Innenministerium gewandt. Eine Antwort steht noch aus.

7 Justiz

7.1 Gesetzgebungsverfahren

7.1.1 Untersuchungshaftvollzugsgesetz

Bereits im August 1996 war durch das Bundesministerium der Justiz ein Referentenentwurf zur **Regelung des Rechts der Untersuchungshaft** erarbeitet worden, später folgte ein Gesetzentwurf der Bundesregierung. Die Bereitschaft zur Erfüllung der von mir schon seit Jahren erhobenen Forderung nach einer gesetzlichen Regelung habe ich begrüßt. Für den Bereich der allgemeinen Datenschutzbestimmungen nahm der Entwurf auf die Regelungen des **Strafvollzugsgesetzes** Bezug, über dessen Novellierung ich in meinem 18. Tätigkeitsbericht unter Nr. 7.1.4 berichtet habe. Darüber hinaus habe ich in einer Stellungnahme zum Entwurf gegenüber dem Bayerischen Staatsministerium der Justiz die Berücksichtigung folgender Punkte gefordert:

- der Untersuchungsgefangene sollte von der Überwachung seines Schriftverkehrs sowie etwa geführter Telefonate unterrichtet werden

- bei der Überwachung des Schriftverkehrs und von Besuchen sollten für den Kontakt mit nahen Angehörigen im Hinblick auf den Schutz von Ehe und Familie auch Ausnahmen möglich sein

- Auskunft über den Aufenthalt in Untersuchungshaft sollte nur gegenüber öffentlichen Stellen zugelassen werden. Diese sollten - falls ihnen Auskunft erteilt wurde - im Falle eines Freispruchs, einer Nichteröffnung oder einer nicht nur vorläufigen Einstellung des Verfahrens hiervon ebenfalls informiert werden

Nach einer Empfehlung des Rechtsausschusses des Bundesrates, in der wesentliche Verschlechterungen zu Lasten des Datenschutzes befürwortet wurden, haben die Datenschutzbeauftragten des Bundes und der Länder am 16.08.1999 eine Entschließung zur Novellierung des **Untersuchungshaftvollzugsgesetzes** gefasst (Anlage). Der Bundesrat hat im Wesentlichen entsprechend der oben angegebenen Empfehlungen votiert. Eine Gegenäußerung der Bundesregierung auf die Empfehlungen des Bundesrates ist bisher nicht erfolgt.

7.1.2 Aktenübermittlung beim Täter-Opfer-Ausgleich

Bereits in meinem 18. Tätigkeitsbericht (Nr. 7.3.2) habe ich über die datenschutzrechtliche Problematik bei der Durchführung des Täter-Opfer-Ausgleichs berichtet. Ich habe insbesondere dargestellt, dass eine Aktenübersendung an private Ausgleichsstellen ohne vorherige Einwilligung des Beschuldigten, insbesondere aber etwaiger Verletzter mangels Rechtsgrundlage unzulässig ist.

Aufgrund der vom Staatsministerium der Justiz vorgetragenen Einwände, dass eine Herbeiführung der Ausgleichsbereitschaft durch die Ausgleichsstellen ohne vorherige Akteneinsicht nicht möglich sei, habe ich mit den Mitarbeitern einer solchen Stelle sowie einem Vertreter des Justizministeriums ein Gespräch zu der datenschutzrechtlichen Problematik geführt. Ein für alle Seiten annehmbares Ergebnis konnte hierbei nicht erzielt werden.

Im November 1998 legte die Bundesregierung einen Referentenentwurf für ein Gesetz zur strafverfahrensrechtlichen Regelung des Täter-Opfer-Ausgleichs vor. Erst auf mein ausdrückliches Nachfragen leitete mir das Staatsministerium der Justiz diesen im Februar 1999 zu. Der Referentenentwurf sah vor, dass eine Aktenzuleitung an die Ausgleichsstellen von Amts wegen oder auf Antrag dieser Stellen erfolgen könne. Lediglich bei einer ausdrücklichen Verweigerung des Einverständnisses durch das Opfer der Straftat sollte ein Ausgleichsversuch unterbleiben.

Ich habe in meiner Stellungnahme gegenüber dem Staatsministerium der Justiz gefordert, eine Aktenzuleitung an die Ausgleichsstelle nur mit Einwilligung des Verletzten und des Beschuldigten zuzulassen, da nur bei beiderseitigem Einverständnis mit einem Ausgleich zu rechnen und somit nur in diesem Falle eine Aktenzuleitung erforderlich sei. Darüber hinaus habe ich verlangt, für die Unterlagen der Ausgleichsstellen eine Vernichtungsfrist von einem Jahr ab Verfahrensabschluss festzulegen und diese Stellen einer anlassunabhängigen Datenschutzkontrolle zu unterwerfen.

Da der Bundesrat in seiner Stellungnahme zum Gesetzentwurf forderte, dass bei der Einleitung des Ausgleichsverfahrens der entgegenstehende Wille des Opfers nicht berücksichtigt werden sollte, haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 58. Konferenz in

einer Entschließung verlangt, eine Datenübermittlung an die Ausgleichsstelle unter Achtung des Willens und der Eigenverantwortung des Verletzten nur mit dessen Einwilligung zuzulassen (Anlage 13).

In dem **Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs vom 20.12.1999** ist zwar, meinen Forderungen entsprechend, eine enge Zweckbindung und eine Vernichtungsregelung für die Daten der Ausgleichsstelle sowie eine anlassunabhängige Datenschutzkontrolle durch die jeweils zuständige Stelle vorgesehen. Bei privaten Stellen, um die es sich im Regelfall handeln wird, sind dies die Aufsichtsbehörden im privaten Bereich, in Bayern also die Regierungen. Die Aktenzuleitung an die mit der Durchführung des Ausgleichs beauftragte Stelle wurde jedoch bedauerlicherweise auch ohne Einwilligung des Beschuldigten oder des Verletzten zugelassen.

7.1.3 Parlamentarische Kontrolle der akustischen Wohnraumüberwachung

In meinem 18. Tätigkeitsbericht (Nr. 7.1.5) hatte ich über das Gesetzgebungsverfahren zur Einführung des sogenannten **„Großen Lauschangriffs“** berichtet. In dem damals eingeführten Art. 13 Abs. 6 Grundgesetz wurde eine Berichtspflicht der Bundesregierung gegenüber dem Bundestag sowie eine gleichwertige parlamentarische Kontrolle in den Ländern vorgeschrieben.

Das in Bayern zur Umsetzung dieser Verpflichtung erlassene **Gesetz zur Anpassung des Bayerischen Landesrechts an Art. 13 des Grundgesetzes vom 10.07.1998** legt fest, dass die Staatsregierung den Landtag jährlich über Maßnahmen der akustischen Wohnraumüberwachung unterrichtet. Ein vom Landtag gewähltes Gremium soll auf der Grundlage dieses Berichts die parlamentarische Kontrolle ausüben.

Zur Durchführung dieser Kontrolle hat der Bayerische Landtag das **Gesetz zur parlamentarischen Kontrolle der Staatsregierung hinsichtlich der Maßnahmen nach Art. 13 Abs. 3 bis 5 des Grundgesetzes sowie der Tätigkeit des Landesamts für Verfassungsschutz vom 10.02.2000** beschlossen. Der Gesetzentwurf sah vor, ein parlamentarisches Kontrollgremium aus fünf Mitgliedern zu bestimmen, dessen Beratungen geheim sein sollten. In einem Schreiben an den Vorsitzenden sowie an den stellv. Vorsitzenden des Ausschusses für Verfassungs-, Rechts- und Parlamentsfragen habe ich darauf hingewiesen, dass eine ausschließlich nicht-öffentliche Erörterung der Auswirkungen dieser tief greifenden und auch Unverdächtige betreffenden gesetzlichen Befugnis durch ein kleines Gremium mit der Verpflichtung zur Geheimhaltung eine öffentliche Kontrolle nicht sicherstellen würde. Ich habe daher vorgeschlagen, neben der Behandlung von Einzelfällen in einer geheim tagenden Kontrollkommission, entsprechend einer Verfahrensweise im Deutschen Bundestag, auch Berichte der Staatsregierung über die grundsätzlichen Erfahrungen mit dem neu eingeführten Verfahren vorzusehen, die im Plenum des Landtages öffentlich zu diskutieren wären.

Diese Vorschläge wurden in dem Gesetz nicht umgesetzt.

Zur Erfüllung ihrer Berichtspflicht hat die Bundesregierung am 27.12.1999 dem Deutschen Bundestag einen Bericht über den Einsatz des „Großen Lauschangriffes“ zum Zweck der Strafver-

folgung im Jahr 1998 vorgelegt. In einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder den ungenügenden Umfang dieses Berichts kritisiert. Er enthält insbesondere keine Ausführungen über von der Maßnahme betroffene Personen, die nicht Beschuldigte und nicht Inhaber der überwachten Wohnung sind. Darüber hinaus wurde eine gleichwertige Berichterstattung auch bezüglich der zur Gefahrenabwehr veranlassten Maßnahmen gegenüber dem Landesparlament gefordert (Anlage 21). Zwischenzeitlich liegt auch ein Bericht der Bundesregierung für das Jahr 1999 vor, der in der Form dem Bericht für das Jahr 1998 entspricht.

Beide Berichte wurden bisher im Plenum des Bundestages nicht beraten. Das Staatsministerium der Justiz hat mir auf Anfrage mitgeteilt, dass bei seinen statistischen Erfassungen jeder Eigentümer, Mieter oder sonst Nutzungsberechtigte und, sofern hiervon nicht ohnehin umfasst, die Beschuldigten des Verfahrens als von der akustischen Wohnraumüberwachung Betroffene angegeben werden. Nicht erfasst würden damit Personen, die sich nur zufällig in der überwachten Wohnung aufgehalten haben. Ich habe das Staatsministerium der Justiz gebeten, klarzustellen, dass der Begriff der „Nutzungsberechtigten“ alle Personen umfasst, die in diesen Räumen wohnen.

7.1.4 Bayerisches Schlichtungsgesetz

Der Landtag hat am 13.04.2000 das **Bayerische Schlichtungsgesetz** beschlossen, wonach einem Verfahren vor dem Zivilgericht bei bestimmten Streitigkeiten ein Schlichtungsverfahren bei einer Schlichtungsstelle zwingend vorauszugehen hat. Schlichtungsstellen sind Notare, Rechtsanwälte oder andere dauerhaft eingerichtete Schlichtungsstellen, die als Gütestellen durch den Präsidenten des Bayerischen Obersten Landesgerichtes anerkannt werden. Diese Schlichtungsstellen können vor ihnen geschlossene Vergleiche beurkunden, die sodann, nach Erteilung einer entsprechenden Klausel, vollstreckbar sind.

Der Recht suchende Bürger, der diese Stellen vor einem Zivilrechtsstreit aufsucht, offenbart dort in der Regel eine Vielzahl von persönlichen Informationen. Ich habe daher gegenüber dem Justizministerium gefordert, in dem Gesetz eine besondere Verschwiegenheitspflicht des mit der Schlichtung betrauten Personals sowie eine möglichst kurze Vernichtungsfrist für die dabei er-

langten Daten festzulegen. Aufgrund des besonderen Angewiesenseins des Bürgers gegenüber der Schlichtungsstelle sowie deren Befugnis, vollstreckbare Vergleiche zu beurkunden, habe ich weiterhin eine Klarstellung im Gesetz gefordert, dass die Schlichtungsstellen eine hoheitliche Aufgabe der öffentlichen Verwaltung wahrnehmen und damit öffentliche Stellen im Sinne des Bayerischen Datenschutzgesetzes sind, die meiner Datenschutzkontrolle unterliegen.

Meine Anregungen wurden im Gesetzgebungsverfahren leider nicht berücksichtigt.

7.1.5 Strafverfahrensänderungsgesetz 1999

Bereits in meinen beiden letzten Tätigkeitsberichten hatte ich über die Gesetzgebungsarbeiten zu einem Strafverfahrensänderungsgesetz berichtet. Im Februar 1999 hat die Bundesregierung einen neuen Entwurf für ein Strafverfahrensänderungsgesetz vorgelegt, der dem Entwurf von 1996 weitgehend entsprach.

In meiner Stellungnahme zu diesem Gesetzentwurf habe ich zunächst darauf hingewiesen, dass auch in dem neuen Entwurf Regelungen zur Aufbewahrung, Aussonderung und Vernichtung der Akten fehlen. Weiterhin habe ich mich insbesondere zu folgenden Bereichen geäußert:

1. Das Recht eines nicht durch Verteidiger vertetenen Beschuldigten auf Akteneinsicht, das auch schon der europäische Gerichtshof für Menschenrechte in einem Frankreich betreffenden Fall gefordert hatte, sollte dem Beschuldigten zwingend zustehen und nicht lediglich im Ermessen der die Akteneinsicht gewährenden Stelle liegen.

2. Längerfristige Observationen sollten nur auf der Grundlage eines richterlichen Beschlusses durchgeführt werden dürfen.

3. Eine enge Zweckbindung, also besondere Beschränkung der Verwendung und Weitergabe, für Erkenntnisse aus besonders eingriffsintensiven Ermittlungen, wie sie bereits für Erkenntnisse aus dem Einsatz von Rasterfahndung, Telefonüberwachung, Abhörmaßnahmen und verdeckten Ermittlern normiert ist, sollte auch für Erkenntnisse aus einer Ausschreibung

zur polizeilichen Beobachtung oder einer längerfristigen Observation gelten.

Nachdem der Bundesrat weitere schwer wiegende datenschutzrechtliche Verschlechterungen gefordert hatte, habe ich mich zusammen mit elf weiteren Landesbeauftragten für den Datenschutz in einer Pressemitteilung sowie in einem Schreiben an die Staatskanzlei und das Justizministerium hiergegen gewandt.
Die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung ebenfalls gegen datenschutzrechtliche Verschlechterungen im Rahmen des Strafverfahrensänderungsgesetzes gewandt (Anlage 16).

Am 08.06.2000 hat der Bundestag eine Beschlussempfehlung des Vermittlungsausschusses zu dem **Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1999** – angenommen. Darin wurde unseren Bedenken insofern Rechnung getragen, als polizeilich veranlasste Öffentlichkeitsfahndungen einer nachträglichen Kontrolle durch die Staatsanwaltschaft unterliegen und eine Öffentlichkeitsfahndung nach Zeugen nur bei Straftaten von erheblicher Bedeutung durchgeführt werden darf. Die darüber hinaus von mir und den anderen Datenschutzbeauftragten des Bundes und Länder geltend gemachten Forderungen, u.a. ausdrückliche gesetzliche Regelung für längerdauernde Observationen schon ab einem Tag, Akteneinsicht für private Dritte nur bei rechtlichem, nicht schon bei bloß berechtigtem Interesse, fanden in dem Gesetz bedauerlicherweise keine Umsetzung.

7.1.6 Zustellungsreformgesetz

Seit Anfang 1997 ist ein Entwurf für ein **Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren** in Bearbeitung. Ich habe in mehreren Stellungnahmen gegenüber dem Staatsministerium der Justiz meine Forderungen hierzu deutlich gemacht. Hierbei ging es vor allem um folgende Punkte:

1. Für die **öffentliche Zustellung** durch Gerichtsaushang sollte ausdrücklich festgestellt werden, dass diese als letztes Mittel nur zulässig ist, wenn keine andere Form der Zustellung, etwa an einen Prozessbevollmächtigten, möglich ist.

2. Die **öffentliche Zustellung** sollte durch Aushang lediglich einer Benachrichtigung und nicht mehr eines Auszuges des gesamten zuzustellenden Schriftstückes erfolgen.

3. In den Entwürfen war für den Schriftverkehr mit Personen, „bei denen aufgrund ihres Berufes von einer erhöhten Zuverlässigkeit ausgegangen werden kann“, die Möglichkeit einer Zustellung durch **elektronische Datenfernübertragung** vorgesehen. Ich habe mich dafür ausgesprochen, eine derartige Datenübermittlung nur zuzulassen, sofern Authentizität, Integrität und Vertraulichkeit der Daten, etwa im Wege einer elektronischen Signatur und der Verschlüsselung gewährleistet sind. Dies gilt um so mehr, als gerade bei dem bezogenen Personenkreis von der Übermittlung besonders sensibler Daten auszugehen ist, die eines besonderen Schutzes in technischer und organisatorischer Hinsicht bedürfen.

In dem inzwischen vorgelegten Gesetzentwurf der Bundesregierung ist eine öffentliche Zustellung im Fall des unbekannten Aufenthalts des Adressaten nur zugelassen, wenn, meiner Forderung entsprechend, eine anderweitige Zustellung an Vertreter oder Zustellungsbevollmächtigte nicht möglich ist. Der Aushang soll sich auf ein Benachrichtigungsschreiben beschränken.

Als besondere Form der Zustellung an Personen mit besonderer Zuverlässigkeit sieht auch der Gesetzentwurf eine Übertragung als Telekopie oder als elektronisches Dokument vor. Die elektronische Datenübertragung soll hierbei mittels einer elektronischen Signatur und einem Schutz gegen unbefugte Kenntnisnahme seitens Dritter gesichert werden. Für die Datenübertragung per

Telekopie besteht eine gleichwertige Sicherungsmöglichkeit nicht. Ich habe bezüglich dieser Übertragungsform daher weiterhin Bedenken im Hinblick auf eine Sicherung von Authentizität, Integrität und Vertraulichkeit.

7.1.7 Elektronisch überwachter Hausarrest

Seit Mai 2000 wird in Hessen die „elektronische Fußfessel“ zur Umsetzung von Bewährungsüberwachungen eingesetzt. Hierbei wird dem Betroffenen für den Lauf seiner Bewährungszeit durch den Richter eine Weisung über einen festgelegten Tagesablauf sowie dessen Kontrolle mittels der elektronischen Fußfessel erteilt. Bereits im Juli 1997 sowie im Juli 1999 hatte es Gesetzentwürfe gegeben, die die Vollstreckung von Freiheitsstrafen mittels eines elektronisch überwachten Hausarrestes bundesweit erlauben sollten. Der Betroffene sollte hierdurch in die Lage versetzt werden, in seinem sozialen Umfeld zu verbleiben und seine materielle Lebensgrundlage zu erhalten.

Der elektronisch überwachte Hausarrest hat große öffentliche Aufmerksamkeit erfahren. Technisch gibt es unterschiedliche Umsetzungsmöglichkeiten. Bei dem derzeit gebräuchlichsten System bestätigt ein am Betroffenen befestigter Sender in bestimmten zeitlichen Abständen den Aufenthalt im Überwachungsbereich eines fest installierten Kontrollgerätes. Das Kontrollgerät sendet dann, permanent oder in bestimmten Intervallen, über die normale Telefonleitung die Bestätigung oder eine Fehlmeldung an die Überwachungseinheit weiter. Es gibt aber bereits technische Lösungen, die in Verbindung mit einem Global Positioning System (GPS) eine aktive Aufenthaltsbestimmung des Betroffenen zulassen. Mit der technischen Einrichtung eines elektronisch überwachten Hausarrestes werden bei den meisten Anwendungen auch die Vereinbarung eines festgelegten Tagesablaufes und regelmäßige Besuche von Vollzugsmitarbeitern sowie Alkohol- und Drogenkontrollen verbunden.

Ich halte den elektronisch überwachten Hausarrest für einen tiefgreifenden Eingriff in das Recht des Betroffenen und seiner Mitbewohner auf informationelle Selbstbestimmung sowie die Unverletzlichkeit der Wohnung. Hinsichtlich des Eingriffs in das Recht auf informationelle Selbstbestimmung des Betroffenen ist allerdings zu berücksichtigen, dass die Ausübung dieses Rechts durch die im Vollzug einer Freiheitsstrafe liegenden Beschränkungen von vorne herein limitiert

ist. Die in der elektronischen Fußfessel als Alternative zum Strafvollzug liegenden Beschränkungen für den Verurteilten werden deshalb in ihrer Relevanz für diesen deutlich relativiert. Gleichwohl erfordert eine solche Maßnahme, soweit sie über einen zeitlich befristeten Modellversuch hinausgeht, eine bereichsspezifische und normenklare gesetzliche Regelung, die Voraussetzungen und Umfang des Eingriffs unter Berücksichtigung dieser Grundrechte festlegt. Dabei sind insbesondere folgende Anforderungen zu berücksichtigen:

- Die Form der Überwachung sollte, entsprechend dem Gebot der Verhältnismäßigkeit, so konzipiert sein, dass sie den Einzelnen unter Berücksichtigung des Vollzugszweckes nur soweit erforderlich belastet. Das gilt sowohl für die Wahl des Überwachungssystems als auch eventuell begleitender Überwachungsmaßnahmen, bei denen insbesondere auf den Schutz sensibler, wie z. B. dem Arzt- oder Sozialgeheimnis unterliegender Daten Rücksicht zu nehmen ist.

- Die Maßnahme sollte nur mit einer aufgeklärten Einwilligung des Betroffenen sowie sämtlicher einsichtsfähiger Mitbewohner stattfinden.

- Die erhobenen Daten sollen sobald sie für die Maßnahme nicht mehr erforderlich sind wieder gelöscht werden.

- Es ist auf eine enge Zweckbindung sowie eine technische und organisatorische Sicherung der Daten gegen den Zugriff Dritter zu achten.

7.2 Datenschutz bei der Strafverfolgung

7.2.1 Aufbewahrungsbestimmungen Strafakten

Obwohl die Datenschutzbeauftragten des Bundes und der Länder, schon auf ihrer 49. Konferenz im Jahre 1995 eine gesetzliche Regelung zur Aufbewahrung und Speicherung von Daten im Justizbereich gefordert haben, sind bis heute Aufbewahrungsfristen für Akten der Zivil- und Strafjustiz lediglich in bundeseinheitlichen Verwaltungsvorschriften der Landesjustizverwaltungen festgelegt. Das OLG Frankfurt a. Main hat am 16.08.1998 (NJW 1999, 73) entschieden, dass die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss des Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch ein formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf. Dabei hat es ausgeführt, dass der Zustand einer fehlenden gesetzlichen Grundlage für die Aufbewahrung von Akten für eine Übergangsfrist zwar noch hinzunehmen sei, dass dies jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei.

Auf dieses Urteil hin ist mir keine gesetzgeberische Initiative bekannt geworden. Auch das Strafverfahrensänderungsgesetz 1999, das zwar Bestimmungen zu Speicherungsprüffristen für Dateien und über den Umgang mit Akten, insbesondere Fragen der Auskunftserteilung und Akteneinsicht enthält, enthält keine Bestimmung über die Aufbewahrungsdauer von Strafakten.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher auf ihrer 58. Konferenz erneut in einer Entschließung gefordert, unverzüglich mit der Schaffung gesetzlicher Regeln über die Aufbewahrung von gerichtlichen Akten der Zivil- und Strafjustiz zu beginnen (Anlage 14).

7.2.2 Mitteilungen an das Wählerverzeichnis

Nach Nr. 12 der neugefassten Mitteilungen in Strafsachen (**Mitteilung zum Wählerverzeichnis**) ist der zuständigen Verwaltungsbehörde die Tatsache einer rechtskräftigen Verurteilung ohne Angabe der rechtlichen Bezeichnung der Tat und ohne Angabe der angewendeten Strafvorschriften mitzuteilen, sofern diese zu einem Verlust der Fähigkeit, öffentliche Ämter zu bekleiden oder Rechte aus öffentlichen Wahlen zu erlangen, oder des Rechts, in öffentlichen Angelegenheiten zu wählen oder zu stimmen, geführt hat. In den Fällen der ausdrücklichen Aberkennung dieser Fähigkeiten oder Rechte ist auch die Zeit mitzuteilen, für die die Aberkennung wirksam ist. Werden vorstehend bezeichnete Fähigkeiten und Rechte wieder verliehen, so ist diese Tatsache in gleicher Weise mitzuteilen.

Das Staatsministerium der Justiz vertrat hierzu die Auffassung, der Verwaltungsbehörde sei lediglich die vom Gericht bestimmte Dauer des Rechtsverlusts, nicht aber dessen Endzeitpunkt, der sich nach der Dauer der Strafvollstreckung bemisst, mitzuteilen. Etwas anderes ergebe sich nur im Fall einer vorzeitigen Wiederverleihung der bezeichneten Fähigkeiten und Rechte. Die Verwaltungsbehörden hätten die Möglichkeit, im Wege einer Einzelabfrage beim Bundeszentralregister zu erfragen, ob der Betroffene zum Zeitpunkt der jeweiligen Wahl im Besitz der genannten Fähigkeiten und Rechte ist.

Nach meiner Auffassung besteht eine Verpflichtung der Justiz, der Verwaltungsbehörde eine Folgemitteilung über den errechneten Endzeitpunkt des Rechtsverlustes zu machen. Dies ergibt sich bereits aus der Vorschrift, die Zeit mitzuteilen, für die die Aberkennung wirksam ist. Durch eine Einzelabfrage beim Bundeszentralregister würden die Verwaltungsbehörden eine unbeschränkte Auskunft erhalten, die eine unverhältnismäßige Datenübermittlung darstellte, die dem Ziel einer beschränkten Auskunft, wie sie in Nr. 12 der Mitteilung in Strafsachen vorgeschrieben ist (ohne rechtliche Bezeichnung der Tat und ohne Angabe der angewendeten Strafvorschriften), widerspräche und die für die Aufgabenerfüllung der Verwaltungsbehörde nicht erforderlich wäre. Im Übrigen scheint mir nicht gesichert, dass die Verwaltungsbehörden tatsächlich in jedem Fall diese Einzelanfragen stellen würden.

Der Mistra-Ausschuss der Landesjustizverwaltungen hat dem Vorschlag, die Anordnung über Mitteilungen in Strafsachen entsprechend zu ändern, zugestimmt. Dabei werte ich es als Erfolg meiner Arbeit, dass auch das Staatsministerium der Jusitz, nachdem es zuvor keine Kompromißbereitschaft hatte erkennen lassen, im MiStra-Ausschuss für eine Änderung der Mitteilungen in Strafsachen votiert hat.

7.2.3 DNA-Analyse

7.2.3.1 DNA-Identitätsfeststellung zur Strafverfolgung

1. Überblick

   Über das Gesetzgebungsverfahren zur Schaffung einer gesetzlichen Grundlage für die Durchführung einer DNA-Analyse zu Strafverfolgungszwecken und deren Speicherung hatte ich in meinem 18. Tätigkeitsbericht (Nr. 7.1.7) berichtet. In diesem **DNA-Identitätsfeststellungsgesetz** wurde festgelegt, dass die Entnahme von Körperzellen sowie deren molekulargenetische Untersuchung durch einen Richter anzuordnen sind und nur bei Straftaten von erheblicher Bedeutung in Betracht kommen. Der Richter muss, sofern die Untersuchung zum Zweck zukünftiger Strafverfahren durchgeführt werden soll, in einer Prognoseentscheidung darüber befinden, ob Grund zu der Annahme besteht, dass gegen den Betroffenen künftig erneut Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sein werden.

2. Umsetzung und datenschutzrechtliche Beurteilung

   Bereits im Vorfeld des Inkrafttretens dieses Gesetzes haben sich insbesondere die Staatsministerien der Justiz und des Innern um eine zügige Umsetzung der neu geschaffenen Befugnisse gerade bei Strafgefangenen und im Maßregelvollzug befindlichen Personen gesorgt. Dabei waren sie von Anfang an bestrebt, die Probenentnahmen und Analysen auf der Grundlage einer Einwilligung des Betroffenen, also ohne richterlichen Beschluss durchzuführen. Hierfür wurde in Anweisungen an die Vollzugsbediensteten darauf hingewiesen, dass

den Betroffenen eine freiwillige Abgabe nahe zu legen sei und dass im Falle einer Verweigerung des Einverständnisses insbesondere die Frage der Gewährung von Vollzugslockerungen oder Urlaub aus der Haft besonders sorgfältig zu prüfen sei.

Ich habe vor allem gegenüber dem Staatsministerium der Justiz deutlich gemacht, dass ich erhebliche Zweifel habe, ob die Einwilligung des Betroffenen eine ausreichende Grundlage für die DNA-Analyse sein kann. Der Gesetzgeber hat für die Durchführung dieser Untersuchung eine richterliche Anordnung auf der Grundlage einer Prognose über künftige Strafverfahren gegen den Betroffenen verlangt. Diese Schutzmechanismen dürfen nicht durch die systematische Einholung von Einwilligungen der Betroffenen umgangen werden. Darüber hinaus ergeben sich gravierende Zweifel an der Freiwilligkeit einer Einverständniserklärung von Personen, die sich in einem Zwangsverhältnis wie dem Strafvollzug oder dem Maßregelvollzug befinden und Auswirkungen ihrer Entscheidung auf Vollzugslockerungen befürchten. Hinzu kommt bei Betroffenen im Maßregelvollzug das Fehlen einer kompetenten Prüfung ihrer Einwilligungsfähigkeit. Jedenfalls hat mir das Innenministerium, das die Einholung der Einverständniserklärungen von der Polizei durchführen lässt, trotz wiederholter Anfragen seit nunmehr einem guten halben Jahr keine Auskünfte dazu erteilt.

Dessen ungeachtet werden weiterhin Probenuntersuchungen aufgrund der Einwilligung durchgeführt und deren Ergebnis in der beim Bundeskriminalamt errichteten DNA-Analysedatei gespeichert.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 58. Konferenz eine Entschließung gefasst, in der sie deutlich gemacht haben, dass die Durchführung einer DNA-Analyse zu Zwecken der Strafverfolgung ohne richterliche Anordnung insbesondere bei Strafgefangenen der gesetzlichen Vorgabe widerspricht (Anlage 9).

Das Staatsministerium der Justiz hat meinen Bedenken nur in Randbereichen Rechnung getragen, als es gegenüber den Justizvollzugsanstalten darauf hingewiesen hat, dass eine Verweigerung des Einverständnisses nur so lange Auswirkungen auf die Gewährung von Vollzugslockerungen haben kann, bis ein richterlicher Beschluss über die Probenentnahme und – untersuchung erholt und ggf. durchgesetzt wurde. Darüber hinaus soll die Einholung der Einverständniserklä-

rung beim Strafgefangenen nicht mehr von Vollzugsbediensteten sondern von Polizeibeamten vorgenommen werden. Diese Verfahrensänderungen stellen aus meiner Sicht eine gewisse Verbesserung dar. Sie räumen aber meine grundsätzlichen Bedenken gegen ein von den gesetzlichen Vorgaben abweichendes Verfahren nicht aus. Von einer Beanstandung habe ich lediglich deshalb abgesehen, weil in einzelnen Entscheidungen von Landgerichten die genannte Verfahrensweise für rechtmäßig angesehen wurde. Andere Landgerichte halten sie dagegen für rechtswidrig. Ich behalte mir eine Beanstandung deshalb ausdrücklich vor.

7.2.3.2 Hinweis auf DNA-Analyse auf Ladungskuvert

Ein Petent hatte mir mitgeteilt, dass er zur Abgabe einer Speichelprobe geladen worden sei. Das hierfür durch die Polizeidienststelle verwendete Kuvert trug auf der Außenseite bei der Absenderangabe den handschriftlichen Vermerk „AG-DNA-Altfälle“. Ich habe der Polizei mitgeteilt, dass diese Beschriftung dem Datenschutz widerspricht. Durch diesen Vermerk ist für Dritte bereits von außen erkennbar, dass die Polizei an den Betroffenen im Rahmen der Erhebung einer DNA-Analyse herantritt, die nach dem Gesetz mit der Erwartung künftiger Straftaten von erheblicher Bedeutung verbunden ist.

Die Polizeidienststelle hat meiner Auffassung entsprochen und verwendet die zur Vereinfachung des Postrücklaufes angebrachte Beschriftung nicht mehr.

7.2.4 Fernmeldegeheimnis

7.2.4.1 TÜ-Abschriften in Sonderbänden

§ 100 b Abs. 6 StPO sieht vor, dass die durch eine Telefonüberwachung erlangten Unterlagen unverzüglich und unter Aufsicht der Staatsanwaltschaft zu vernichten sind, sobald sie zur Strafverfolgung nicht mehr erforderlich sind. Anlässlich einer Überprüfung der Umsetzung dieser Vorschrift habe ich festgestellt, dass eine einheitliche Handhabung nicht besteht. Ich habe gegenüber dem Staatsministerium der Justiz auf eine Klarstellung gedrungen, wie lange die Aufbewahrung von Unterlagen, die bei der Telefonüberwachung gewonnen wurden, zur Strafverfolgung erforderlich ist. Hierbei habe ich deutlich gemacht, dass eine Aufbewahrung nach rechtskräftigem Abschluss des Verfahrens allein im Hinblick auf die theoretische Möglichkeit eines Wiederaufnahmeverfahrens im Widerspruch zu der gesetzlichen Regelung stünde.

Das Justizministerium hat auf eine übereinstimmende Regelung für sämtliche Oberlandesgerichtsbezirke in Bayern hingewirkt, nach der schriftliche Aufzeichnungen von Telefongesprächen in Sonderbänden abzuheften sind. Abschriften über einzelne Telefongespräche mit Beweisfunktion sind in die Ermittlungsakten aufzunehmen. Nach Rechtskraft des Urteils sind die bespielten Tonträger zu löschen und die Sonderbände zu vernichten. In den Ermittlungsakt aufgenommene Abschriften werden erst zusammen mit diesem vernichtet.

Dieses Verfahren stellt eine Verbesserung des Datenschutzes dar.

7.2.4.2 Dokumentation von TÜ-Materialien bei der Staatsanwaltschaft

In seinem Urteil vom 14.07.1999 zur Fernmeldeüberwachung durch den Bundesnachrichtendienst (siehe Nr. 6.2.7) hat das Bundesverfassungsgericht eine Dokumentation aller Fälle der Weitergabe oder zweckändernden Nutzung der durch einen Eingriff in das Fernmeldegeheimnis erlangten Daten verlangt. Die Pflicht, die Daten zu kennzeichnen und deren Weitergabe zu protokollieren, besteht, um eine hinreichende Kontrolle der Speicherung, Zweckänderung und Übermittlung zu gewährleisten.

Wie ich anläßlich einer Prüfung erfahren habe, hält zumindest eine Staatsanwaltschaft eine lückenlose Dokumentation von Abschriften für nicht möglich. Ich habe mich daher an das Staatsministerium der Justiz gewandt und auf die durch das Bundesverfassungsgericht geforderte Dokumentationspflicht hingewiesen, durch die der Schutz des Fernmeldegeheimnisses sichergestellt werden soll.

Eine Antwort des Staatsministeriums der Justiz steht noch aus.

7.2.4.3 Benachrichtigung Beteiligter

Nach § 101 Abs. 1 StPO sind im Fall einer Telefonüberwachung die Beteiligten hiervon zu benachrichtigen, sobald dies ohne Gefährdung insbesondere des Untersuchungszweckes geschehen kann. Als Beteiligte kommen, neben dem Beschuldigten und einem eventuell personenverschiedenen Anschlussinhaber, alle Personen in Betracht, mit denen der Beschuldigte den überwachten Fernmeldeverkehr unterhalten hat. Hierbei ist jedoch zu berücksichtigen, dass die Benachrichtigung selbst zu einer Beeinträchtigung des informationellen Selbstbestimmungsrechtes des Beschuldigten oder des Anschlussinhabers führen kann, wenn Dritte erst durch die Benachrichtigung von der erfolgten Telefonüberwachung und damit von der Tatsache eines gegen den Beschuldigten gerichteten Strafverfahrens erfahren. Eine Information sollte aber gegenüber solchen Gesprächsteilnehmern erfolgen, deren Gespräche für beweiserheblich befunden und daher in den Ermittlungsakt aufgenommen wurden.

Anlässlich der Prüfung einer Staatsanwaltschaft habe ich festgestellt, dass der Pflicht zur Benachrichtigung des Beschuldigten und des Anschlussinhabers, wie auch anderer Gesprächsteilnehmer, deren Gespräch im Ermittlungsakt dokumentiert war, wiederholt nicht nachgekommen wurde. Ich habe daher verlangt, die Sachbearbeiter ggf. durch die Verwendung eines auszufüllenden Formblattes auf die gesetzliche Verpflichtung hinzuweisen.

Eine Stellungnahme hierzu steht noch aus.

7.2.4.4 Forschungsvorhaben zur Auswertung von TÜ-Maßnahmen

Bereits in meinem 17. Tätigkeitsbericht (Nr. 7.4.3.7) hatte ich von meiner Forderung nach einer Auswertung der Telefonüberwachungsmaßnahmen im Hinblick auf deren Erfolg berichtet. Auch die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat erneut eine Überprüfung dieser staatlichen Befugnisse auf ihre Effektivität im Verhältnis zur Intensität des Eingriffs gefordert.

In diesem Sinn hat das Bundesministerium der Justiz am 20.08.1999 ein **Forschungsvorhaben zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO“** ausgeschrieben und an das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg vergeben. Im Rahmen dieses Forschungsvorhabens sollen tatsächliche Erkenntnisse zur Bewertung der Notwendigkeit und Erfolgseignung von Fernmeldeüberwachungsmaßnahmen gewonnen werden, wobei auch geprüft werden soll, in welchem Umfang unbeteiligte Dritte von der Maßnahme betroffen werden.

7.3 Gerichtlicher Bereich

7.3.1 Mitteilungen in Zivilsachen (MiZi)

Wie in meinem 18. Tätigkeitsbericht (Nr. 7.1.1) geschildert, wurden die Befugnisse von Gerichten und Staatsanwaltschaften, von Amts wegen personenbezogene Daten an öffentliche Stellen zu übermitteln, durch das **Justizmitteilungsgesetz vom 18. Juni 1997** geregelt. Aufgrund der veränderten Rechtslage haben die Justizverwaltungen der Länder den Entwurf einer Neuregelung der **Anordnung über Mitteilungen in Zivilsachen** erarbeitet. Zu dem Entwurf habe ich mich in Abstimmung mit den anderen Datenschutzbeauftragten des Bundes und der Länder in einer Stellungnahme geäußert. Ich habe vor allem verlangt, die Mitteilungen regelmäßig auf den Entscheidungstenor zu beschränken und eine detaillierte Dokumentation der Mitteilungen vorzuschreiben. Ein besonderes Anliegen war mir, dass ein Betroffener über Mitteilungen, die aufgrund einer Ermessensentscheidung erfolgen, zwingend informiert wird. Gerade in diesen Fällen, in denen der Betroffene nichts von der Mitteilung weiss und auch nicht wissen kann, gebietet es das Recht auf informationelle Selbstbestimmung sowie der Grundsatz eines fairen Rechtsschutzes, dass er von der Datenübermittlung unterrichtet wird.

Diese Vorschläge wurden, obwohl sie von sämtlichen Datenschutzbeauftragten geteilt wurden, in der Neufassung der Anordnung über Mitteilungen in Zivilsachen, die am 01.06.1998 in Kraft trat, nicht berücksichtigt. Nur in Fällen der Mitteilungen in Betreuungssachen zur Gefahrenabwehr und zur Verfolgung von Straftaten und Ordnungswidrigkeiten wurde eine detaillierte Dokumentation vorgeschrieben. Auch eine Information des Betroffenen von der Mitteilung wurde lediglich für den Fall der Mitteilung an den Träger der Sozialhilfe über eine Kündigungsklage wegen Zahlungsunfähigkeit vorgeschrieben. Für die Fälle einer auf einer Ermessensentscheidung beruhenden Mitteilung wurde davon abgesehen.

Auch im Rahmen einer erneuten Änderung der MiZi zur Anpassung an das seit 01.01.1999 geltende Insolvenzverfahren habe ich eine Information des Betroffenen von der Mitteilung gefordert, sofern diese nicht zwingend, sondern aufgrund einer Ermessensentscheidung erfolgte. Auch in diesem Fall wurden meine Anregungen nicht umgesetzt.

7.3.2 Akteneinsicht eines ehemals Betreuten in den Betreuungsakt

Ein Bürger hatte sich an mich gewandt, da ihm eine Einsicht in die Gerichtsakten, die eine bereits abgeschlossene Betreuung seiner Person betrafen, durch das Gericht mehrfach mit dem Hinweis auf die fehlende Glaubhaftmachung eines berechtigten Interesses verweigert worden war. Ich habe dem Gericht daraufhin mitgeteilt, dass der Betroffene als Verfahrensbeteiligter bereits aufgrund dieser Stellung ein berechtigtes Interesse an der Akteneinsicht hat, das nicht zusätzlich glaubhaft zu machen ist. Das Gericht hat die beantragte Akteneinsicht dementsprechend gewährt.

7.3.3 Presserichtlinien

Bereits in meinem 18. Tätigkeitsbericht (Nr. 7.4.5) habe ich über meine Vorschläge zur Neufassung der **Richtlinien für die Zusammenarbeit der Bayerischen Justiz mit der Presse** berichtet. Zu den von mir im einzelnen dargelegten Punkten konnte weitgehende Einigkeit erzielt werden. Insbesondere wurde aufgenommen, dass gegenüber dem Auskunftsanspruch der Presse stets das Persönlichkeitsrecht der Betroffenen als verfassungsrechtlich geschütztes Rechtsgut zu berücksichtigen ist.

Auch die folgende Überarbeitung der Presserichtlinien wurde mir zur Kenntnis gebracht. In diesem Rahmen habe ich vor allem noch auf folgende Punkte hingewiesen:

1. Personenbezogene Daten sollen bei einer Berichterstattung in Strafsachen nur ausnahmsweise weitergegeben werden. Dies gilt auch für weitere Angaben, durch die eine Identifizierung der Betroffenen ermöglicht würde.

2. Eine aktive Öffentlichkeitsarbeit muss, sofern sie personenbezogen erfolgt, restriktiv gehandhabt werden. Hierbei ergibt sich gerade aus der Unschuldsvermutung vor Verurteilung eine besondere Verpflichtung zur Neutralität. Wertungen zu Lasten des Betroffenen sind deshalb zu unterlassen.

3. Zur Unterrichtung über allgemein interessierende Zivilverfahren werden durch die Gerichte geeignet erscheinende Entscheidungen an die Justizpressestellen bei den Oberlandesgerichten sowie das Pressereferat des Staatsministeriums der Justiz weitergeleitet. Ich habe gefordert, diese justizinterne Weiterleitung nur in anonymisierter Form zuzulassen.

Das Staatsministerium der Justiz hat meine Forderung zu 1 und 2 akzeptiert, zu meiner Forderung zu 3 technische Schwierigkeiten geltend gemacht, die eine Berichterstattung wesentlich erschweren würden. Ich habe es akzeptiert, dass die Entscheidungen bis zur Behebung der technischen Probleme lediglich im Rubrum und gegebenenfalls im Tenor anonymisiert übermittelt werden.

7.3.4 Online-Abruf von Grundbuchdaten

Seit 1994 gibt es in Bayern, ausgehend vom Amtsgericht München, ein maschinell geführtes Grundbuch bei dem die Einsichtnahme, soweit vom Gesetz zugelassen, im Wege eines automatisierten Abrufverfahrens erfolgen kann. Im Rahmen dieses Verfahrens wird das nach der Grundbuchordnung für die Einsichtnahme darzulegende berechtigte Interesse in Form einer so genannten „Darlegungserklärung“ mit den formularmäßigen Gründen „eigene Berechtigung am Grundstück“, „Zustimmung des Eigentümers“ oder „Zwangsvollstreckung“ bei der Anfrage eingegeben. Wie auch die übrigen Eingaben des Abrufs wird diese Erklärung protokolliert.

Behörden, Notare und öffentlich bestellte Vermessungsingenieure sind bei der Grundbucheinsicht von der Darlegung des öffentlichen Interesses befreit. Aber auch bei deren Abrufen werden die abrufende Person/Stelle, Aktenzeichen, Datum des Abrufs und ausgegebenes Grundbuchblatt protokolliert. Zur Kontrolle, ob diese Abrufe nur bei Vorliegen eines berechtigten Interesses durchgeführt wurden, habe ich bei einer Behörde anhand der protokollierten Daten eine stichprobenartige Überprüfung vorgenommen. Hierbei konnte ich keine missbräuchliche Nutzung des automatisierten Abrufverfahrens feststellen.

7.4 Justizvollzugsanstalten

7.4.1 Briefkontrolle

1. Brieföffnung bei bereits Entlassenen

Durch eine Eingabe habe ich erfahren, dass in einer Justizvollzugsanstalt Briefe an einen bereits aus der Haft Entlassenen, die trotz Nachsendeantrages bei der Justizvollzugsanstalt eingegangen waren, nach dem Eingang geöffnet wurden. Nach der Öffnung wurden sie mit Heftklammer und Klebestreifen wieder verschlossen und an die neue Adresse nachgesandt.

Auf mein Einschreiten hin hat die Justizvollzugsanstalt in einer Dienstanweisung darauf hingewiesen, dass eingehende Briefe an bereits aus der Haft Entlassene nicht geöffnet werden dürfen. Im Fall einer dennoch erfolgten versehentlichen Öffnung sei der Brief in einem zusätzlichen Umschlag, der keinen Rückschluss auf die Inhaftierung zulässt, zu verschließen und an die neue Adresse nachzusenden.

2. Schreiben der Staatsanwaltschaft in Sammelumschlägen

Bei der anlaßbezogenen Kontrolle der Briefüberwachung einer Justizvollzugsanstalt habe ich festgestellt, dass Schreiben der Staatsanwaltschaft, in deren Zuständigkeitsbereich die Justizvollzugsanstalt liegt, an dort Inhaftierte in einem Sammelumschlag ohne weitere Sicherung der einzelnen Schriftstücke geschickt werden. In der Justizvollzugsanstalt werden die Schreiben dann nach Adressaten sortiert und an diese ausgehändigt.
Ich habe sowohl die Justizvollzugsanstalt als auch die Staatsanwaltschaft darauf hingewiesen, dass die Justizvollzugsanstalt durch diese Verfahrensweise zwangsläufig vom Inhalt der einzelnen Schreiben Kenntnis nehmen kann. Eine Überwachung des Briefverkehrs darf aber nach den gesetzlichen Bestimmungen nur für den Einzelfall aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erfolgen. Die Notwendigkeit, Schreiben der Staatsanwaltschaft aus diesen Gründen generell zu überwachen, kann ich nicht erkennen. Ich habe deshalb die Staatsanwaltschaft aufgefordert, ihre Praxis zu ändern und Schreiben an Inhaftierte jeweils in gesonderten Umschlägen zu verschicken.

Eine Stellungnahme hierzu steht noch aus.

7.4.2 Praxis der Besucherüberprüfung

Wie ich in meinem 17. Tätigkeitsbericht (Nr. 7.3.2.10) berichtet habe, werden - soweit es von der Justizvollzugsanstalt für erforderlich gehalten wird - bei Polizei/Staatsanwaltschaft/Verwaltungsbehörden Erkundigungen über potenzielle Besucher eingeholt. Grundlage war die Einverständniserklärung des Betroffenen, ohne die er zum Besuch nicht zugelassen wurde.

Aufgrund der seit 01.12.1998 wirksamen Novellierung des Strafvollzugsgesetzes können die Justizvollzugsanstalten nunmehr Daten über Dritte auch ohne deren Mitwirkung erheben, sofern dies für die Behandlung eines Gefangenen, die Sicherheit der Anstalt oder die Sicherung des Vollzuges einer Freiheitsstrafe unerlässlich ist und die Art der Erhebung schutzwürdige Interessen des Betroffenen nicht beeinträchtigt. Aufgrund einer Eingabe habe ich festgestellt, dass trotz der geänderten Rechtslage zumindest in einer Justizvollzugsanstalt weiterhin ein Formblatt verwendet wurde, in dem der potenzielle Besucher sein Einverständnis mit der Einholung von Auskünften über ihn bei den zuständigen Behörden geben kann. Diese Einverständniserklärung war nach dem Wortlaut des Formblatts Voraussetzung für die Entscheidung der Justizvollzugsanstalt über die Zulassung als Besucher.

Ich habe mich an das Staatsministerium der Justiz gewandt und dargelegt, dass es angesichts der geänderten Rechtslage nicht angehen könne, die Entscheidung der Justizvollzugsanstalt über einen Besuchsantrag vom Einverständnis des Antragstellers mit seiner Überprüfung abhängig zu machen. Das Staatsministerium hat daraufhin mitgeteilt, dass das Formblatt geändert werde. Auch die Formblätter anderer Justizvollzugsanstalten würden, sofern solche überhaupt Verwendung finden, entsprechend angepasst werden.

In dem geänderten Formblatt war weiterhin die Abgabe einer Einverständniserklärung vorgesehen, wobei der Zusatz, dass die Zustimmung Voraussetzung für die Zulassung als Besucher sei, weggelassen wurde. Dennoch könnte der Antragsteller aufgrund des Hinweises auf eine evtl. Notwendigkeit der Einholung von Auskünften davon ausgehen, dass eine Verweigerung des

Einverständnisses automatisch zur Ablehnung des Besuchsantrages führt und diese nur deswegen erklären. Andererseits würde der Bürger, der glaubt, ihm werde die Entscheidung über die Datenerhebung und Verarbeitung überlassen, irregeführt, wenn im Falle seiner Weigerung die für eine Zulassungsentscheidung erforderlichen Informationen ohne seine Kenntnis von Amts wegen erhoben werden. Wegen einer Neufassung bin ich mit dem Justizministerium noch im Gespräch.

7.4.3 Weitergabe ärztlicher Daten an die vorgesetzte Behörde

In den im Jahr 1998 neu geschaffenen Bestimmungen des Strafvollzugsgesetzes über die Datenverarbeitung wurden auch Regelungen aufgenommen, die den Schutz besonders sensibler personenbezogener Daten gewährleisten sollen, insbesondere solcher, die einer beruflichen Schweigepflicht unterliegen.

Ich habe in einer Stellungnahme an das Staatsministerium der Justiz auf die Bedeutung der ärztlichen Schweigepflicht des Anstaltsarztes gegenüber der Dienstaufsicht hingewiesen:

- Offenbarungen von Ärzten dürfen grundsätzlich nur gegenüber dem Anstaltsleiter und nur unter den engen gesetzlichen Voraussetzungen für die dort genannten Zwecke (Aufgabenerfüllung der Vollzugsbehörde und Abwehr erheblicher Gefahren für Leib und Leben) erfolgen. Eine Offenbarung gegenüber anderen Vollzugsbediensteten ist nur aufgrund einer Entscheidung des Anstaltsleiters zulässig.

- Die Weitergabe so erlangter Daten durch den Anstaltsleiter an die vorgesetzte Behörde ist an die gleichen Voraussetzungen und Zwecke gebunden wie die Weitergabe durch den Arzt an den Anstaltsleiter.

- Diese Einschränkungen gelten auch für Offenbarungen des Arztes gegenüber der vorgesetzten Behörde.

Jede Weitergabe ärztlicher Daten hat auch das Gebot der Verhältnismäßigkeit zu beachten. Anstelle der Offenbarung dürfen keine anderen Maßnahme zur Verfügung stehen, die, bei gleicher

Wirksamkeit für den verfolgten Zweck, das Recht des Gefangenen auf informationelle Selbstbestimmung geringer beeinträchtigten würden.

Das Staatsministerium der Justiz hat dieser Auffassung grundsätzlich zugestimmt.

7.4.4 Aufbewahrungsbestimmungen Vollzug

Unter Nr. 7.2.1 habe ich über das Fehlen einer gesetzlichen Regelung zur Dauer der Aufbewahrung von Akten der Zivil- und Strafjustiz berichtet. Für den Bereich der Justizvollzugsanstalten wurden mit der Neufassung des Strafvollzugsgesetzes, die am 01.12.1998 in Kraft trat, Aufbewahrungsfristen für Gefangenenpersonalakten, Gesundheitsakten, Krankenblätter und Gefangenenbücher als Höchstfristen festgelegt. Meine Forderung nach einer gesonderten Führung und dementsprechend auch Vernichtung solcher Teile des Gefangenenpersonalakts, die neben der Gesundheitsakte und den Krankenblättern weitere besonders sensible Daten, wie z. B. Unterlagen über psychologische oder sozialtherapeutische Behandlungen oder Erkenntnisse aus der Überprüfung von Besuchern oder der Briefkontrolle enthalten, wurde bedauerlicherweise nicht berücksichtigt.

Anlässlich der geplanten Änderung der bundeseinheitlichen Aufbewahrungsbestimmungen, in denen die Aufbewahrungsfristen für Akten geregelt sind, habe ich mich über die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen an das für die Neufassung federführende dortige Justizministerium gewandt und datenschutzrechtliche Verbesserungen gefordert:

- Für sämtliche in den Aufbewahrungsbestimmungen formulierte Fristen sollte deutlich gemacht werden, dass es sich um Höchstfristen handelt, die nicht überschritten aber, sofern eine weitere Aufbewahrung nicht mehr erforderlich ist, unterschritten werden dürfen.

- Aktenteile mit besonders sensiblen personenbezogenen Daten, wie z. B. Aktenvermerke über Brief- und Telefonüberwachungen, erkennungsdienstliche Unterlagen oder Erkenntnisse über Dritte sollten in Sonderheften des Gefangenenpersonalakts geführt werden und dementsprechend einer eigenen Aussonderungsfrist unterliegen.

Zu letztgenannter Forderung hatte mich auch der Fall eines ehemaligen Untersuchungsgefangenen veranlasst, der in der Untersuchungshaft erkennungsdienstlich behandelt worden war. Nachdem er von dem zugrundeliegenden Vorwurf rechtskräftig freigesprochen worden war, hatte er gefordert, die in der Justizvollzugsanstalt noch vorhandenen erkennungsdienstlichen Unterlagen zu vernichten. Unter Berufung auf die Regelungen des Strafvollzugsgesetzes, hatte die Justizvollzugsanstalt Lichtbilder des Betroffenen sowie eine Beschreibung seiner körperlichen Merkmale weiterhin aufbewahrt und lediglich darüber hinausgehende erkennungsdienstliche Unterlagen vernichtet.

Ich habe hiergegen eingewandt, dass die entsprechende Regelung des Strafvollzugsgesetzes nicht auf Untersuchungsgefangene übertragbar ist, die rechtskräftig freigesprochen wurden. Die weitere Aufbewahrung von Lichtbildern und Beschreibung körperlicher Merkmale ist dort vorgesehen, um spätere Fahndungsmaßnahmen zu erleichtern. Bei einem rechtskräftigen Freispruch verbietet sich aber, auch im Hinblick auf die Unschuldsvermutung, die Prognose einer zukünftigen Fahndung, weshalb eine fortdauernde Speicherung nicht erforderlich und somit unzulässig ist.

Das Staatsministerium der Justiz hat dennoch einer Vernichtung dieser Unterlagen widersprochen, da eine solche Teillöschung einzelner, nicht getrennt geführter Teile des Gefangenenpersonalaktes dem Gebot der Aktenvollständigkeit widersprechen würde.

Im Hinblick auf diese Argumentation habe ich eine getrennte Aufbewahrung in Sonderakten gefordert, die eine vorzeitige Vernichtung bei Wahrung der Integrität der Hauptakte ermöglichen würde. Die Umsetzung dieser Forderung in der Änderung der Aufbewahrungsbestimmungen bleibt abzuwarten.

7.4.5 ADV-Vollzug

In meinem 18. Tätigkeitsbericht (Nr. 7.2.4) habe ich über die Entwicklung eines **Informationssystems über Gefangenendaten** (**ADV-Vollzug**) berichtet. Inzwischen wurde das Verfahren freigegeben und soll bis zum Jahr 2001 in sämtlichen Justizvollsanstalten Bayerns zum Einsatz kommen.

Das dem System zugrunde liegende Konzept berücksichtigt meine Anregungen insofern, als hinsichtlich der Löschung von Gefangenendaten nach Entlassung oder Verlegung in eine andere Anstalt auf die gesetzlich vorgeschriebene Frist von 2 Jahren verwiesen wird, sofern nicht bestimmte Daten zur Auffindung der Gefangenenpersonalakte hiervon ausgenommen sind. Auch wird dem Gefangenen jetzt freigestellt, die Frage nach dem Bekenntnis auf dem Personalblatt zu beantworten oder nicht. Besonders habe ich begrüßt, dass ein Zugriff der Justizvollzugsbediensteten auf personenbezogene Daten der Gefangenen nur soweit gewährt wird, als er für die Erfüllung der dienstlichen Aufgaben erforderlich ist. Dies soll durch ein Rollenkonzept der jeweiligen Justizvollzugsanstalt sichergestellt werden, in dem jeweils Art und Umfang des Zugriffs auf die Daten für die Bediensteten festzulegen ist.

7.5 Ordnungswidrigkeitenverfahren

7.5.1 Fahrerermittlung durch Lichtbildabgleich

Obwohl ich mich in meinen beiden vorangegangenen Tätigkeitsberichten (17. Tätigkeitsbericht Nr. 7.5.4, 18. Tätigkeitsbericht Nr. 7.6.4) zur Frage der Zulässigkeit eines Lichtbildabgleichs mit dem Pass- bzw. Personalausweisregister zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr geäußert hatte, musste ich erneut feststellen, dass insbesondere bei den zur Verfolgung und Ahndung von Verkehrordnungswidrigkeiten berechtigten Gemeinden Unsicherheit in der Frage besteht, unter welchen Voraussetzungen eine Einsichtnahme in die Lichtbilder des Pass- bzw. Personalausweisregisters zulässig ist.

Das Pass- bzw. Personalausweisgesetz setzt für einen Zugriff auf die in den entsprechenden Registern gespeicherten Lichtbilder unter anderem voraus, dass die Daten bei dem **Betroffenen** nicht oder nur mit unverhältmäßig hohem Aufwand erhoben werden können. Betroffener im Sinne dieses Gesetzes ist derjenige, in dessen Recht auf informationelle Selbstbestimmung durch den Zugriff auf „sein“ Lichtbild eingegriffen werden soll. In Bezug auf diese Person muss die Datenerhebung unmöglich oder unverhältnismäßig sein. Ist dies nicht der Fall, hat die Datenerhebung beim Betroffenen Vorrang vor der zweckändernden Nutzung des Lichtbildes.

Es ist deshalb regelmäßig erforderlich, vor dem Zugriff auf das Lichtbild zu versuchen, den Bildabgleich bei dem Betroffenen durchzuführen. Dazu kommt in erster Linie eine mündliche oder schriftliche Aufforderung in Betracht, sich für einen Vergleich mit dem bei der Ordnungswidrigkeit gefertigten Lichtbild einzufinden. Diese Aufforderung stellt keine Anhörung im Sinne des Ordnungswidrigkeitengesetzes dar, sondern gibt dem Betroffenen Gelegenheit, den Zugriff auf das Register durch seine Mitwirkung entbehrlich zu machen. Erst bei Erfolglosigkeit der Aufforderung ist der Zugriff auf das Bild des Pass- bzw. Personalausweisregisters zulässig, soweit die Unmöglichkeit oder Unverhältnismäßigkeit der Datenerhebung beim Betroffenen nicht bereits zuvor feststand. Unverhältnismäßigkeit ist aber grundsätzlich weder aufgrund der Anzahl der in Frage kommenden Betroffenen noch im Hinblick auf die bei Verkehrordnungswidrigkeiten kurze Verjährungsfrist anzunehmen. Eine Aufforderung zur Mitwirkung bei einem Lichtbildabgleich kann relativ kurzfristig erfolgen. Jedenfalls geht es nicht an, die Verjährungsfrist als

Argument für einen generellen Ausschluss der im Pass- bzw. Personalausweisgesetz festgelegten Eingriffsvoraussetzungen zu akzeptieren und damit einer Verkürzung der Betroffenenrechte zuzustimmen.
Umfeldermittlungen z. B. durch Befragung von Nachbarn sind keine Datenerhebungen bei dem Betroffenen selbst, sondern stellen Datenerhebungen bei Dritten dar. Diese sind als intensiverer Eingriff in die Rechte des Betroffenen gegenüber der Datenerhebung beim Betroffenen selbst oder einem Zugriff auf das Lichtbild aus Gründen der Verhältnismäßigkeit nachrangig.

7.5.2 Zusendung von Lichtbildern

Ein Bürger hatte sich an mich gewandt und vorgetragen, er habe im Rahmen eines Verkehrsordnungswidrigkeitenverfahrens einen Anhörungsbogen erhalten. Da zur Tatzeit der Pkw auch von anderen Personen geführt worden sei, habe er in seiner Äußerung um Übersendung des als Beweismittel angegebenen Lichtbildes gebeten. Er habe dabei in die Lage versetzt werden wollen, von seinem Äußerungsrecht Gebrauch zu machen. Statt dem Wunsch zu entsprechen, sei das Bild der für seinen Wohnsitz zuständigen Polizeidienststelle in einem anderen Bundesland zugesandt worden. Diese habe Befragungen in seinem Wohnumfeld durchgeführt.

Ich habe festgestellt, dass die Übersendung der Akten an die Polizei eines anderen Bundeslandes im konkreten Fall unzulässig war. Hier wäre es möglich gewesen, dem äußerungsbereiten Betroffenen das Lichtbild zuzusenden und auf die Datenübermittlung an die Polizei zu verzichten.

Auf mein Schreiben hat das Staatsministerium des Innern mitgeteilt, dass es ihm aufgrund der inzwischen fortgeschrittenen technischen Möglichkeiten in vergleichbaren Fällen „vertretbar“ erscheine, dem aussagebereiten Fahrzeughalter einen Printerabzug des Beweisfotos zuzusenden. Unter Berücksichtigung des Standes der Technik werde geprüft, das Beweisfoto auf den Anhörungsbogen aufzudrucken.

7.6 Sonstiges

7.6.1 Richtlinie für die Förderung der Insolvenzberatung

In dem seit 01.01.1999 geltenden Verbraucherinsolvenzverfahren kann sich der Schuldner bei seinem Antrag auf Eröffnung des Insolvenzverfahrens und bei dem Versuch einer außergerichtlichen Einigung mit den Gläubigern von einer Insolvenzberatungsstelle beraten und vertreten lassen. Diese Stellen erhalten als anerkannte Beratungsstellen in gemeinnütziger und kommunaler Trägerschaft auf Antrag staatliche Zuwendungen, die je nach Anzahl der behandelten Fälle in Form von Pauschalen gewährt werden. Zu Nachweis und Prüfung der einzelnen Fälle durch die Regierungen erstellen die Beratungsstellen einen so genannten **Verwendungsnachweis**, in dem fallbezogen jeweils der Name des Schuldners, die Zahl der Gläubiger, die Gesamthöhe der geltend gemachten Forderungen und weitere Angaben über die geleistete Beratung gemacht werden. Die Übermittlung von Belegen an die Regierungen soll nur noch stichprobenweise erfolgen. Im Rahmen der Neufassung der Richtlinien für die Förderung der Insolvenzberatung durch das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit, habe ich darauf hingewiesen, dass selbst für diese reduzierte Übermittlung von personenbezogenen Daten eine gesetzliche Grundlage nicht besteht und diese daher nur mit Einwilligung des Betroffenen möglich ist. Ich habe daher gefordert, den Verwendungsnachweis, der vom Schuldner unterschrieben wird, um die Erklärung zu erweitern, dass der Schuldner auch in die Datenübermittlung an die zuständige Regierung einwilligt.

Das Staatsministerium hat meiner Forderung entsprochen.

8 Gemeinden, Städte und Landkreise

8.1 Prüfungen

Bei der Prüfung eines Landratsamtes musste ich folgende Mängel feststellen, die - soweit nichts anderes ausgeführt ist - von der betroffenen Stelle dann selbst behoben wurden:

8.1.1 Mängel im Anlagen- und Verfahrensverzeichnis

Jede öffentliche Stelle hat gem. Art. 27 Abs. 1 BayDSG ein Verzeichnis der bei ihr eingesetzten Datenverarbeitungsanlagen und freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, zu führen. Eine bestimmte Form ist dafür nicht vorgeschrieben, es muss jedoch sichergestellt sein, dass die in Art. 27 Abs. 2 i.V.m. Art. 26 Abs. 2 BayDSG genannten Angaben enthalten sind. Nähere Ausführungen zum Inhalt des Anlagen- und Verfahrensverzeichnisses finden sich unter Nr. 5 der Gemeinsamen Bekanntmachung der Bayerischen Staatskanzlei und der Bayerischen Staatsministerien zum Vollzug des Bayerischen Datenschutzgesetzes.

Das von mir überprüfte Landratsamt führte zwar sowohl ein Anlagen- als auch ein Verfahrensverzeichnis. Das Anlagenverzeichnis enthielt jedoch keine Angaben zu der eingesetzten Software (Betriebssystem, Basissoftware, Bezeichnung der auf der Anlage eingesetzten Verfahren, die im Verfahrensverzeichnis enthalten sind; vgl. Nr. 5.2 der Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz). Im Verfahrensverzeichnis waren in der Regel nur der Name des jeweiligen Verfahrens und die Art der gespeicherten Daten aufgeführt. Es fehlten jedoch bei den meisten Verfahren Angaben zu den Aufgaben, zu deren Erfüllung personenbezogene Daten verarbeitet oder genutzt werden, zur Rechtsgrundlage der Verarbeitung und Nutzung, zum Kreis der Betroffenen, zur Art der regelmäßig zu übermittelnden Daten und deren Empfänger, zu den Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung sowie zu den verarbeitungs- und nutzungsberechtigten Personen (vgl. Art. 27 Abs. 2 i.V.m. Art. 26 Abs. 2 BayDSG).

Neben der bereits erwähnten Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz enthält der Kommentar von Wilde/Ehmann/Niese/Knoblauch zum Bayerischen Datenschutzgesetz in den Erläuterungen zu Art. 27 umfassende Ausführungen zu Aufbau, Inhalt und Führung des Anlagen- und Verfahrensverzeichnisses.

8.1.2 Änderung der Passwörter

Durch die Vergabe eines Passwortes soll ein wirksamer Schutz personenbezogener Daten vor der Einsichtnahme durch Dritte erreicht werden. Die Handhabung der Passwortverwaltung des überprüften Landratsamtes war nicht geeignet, dies in allen Bereichen des Landratsamtes zu gewährleisten.

Technische Vorkehrungen, durch die die Mitarbeiter des Landratsamts zum Wechsel ihres Passwortes gezwungen werden, bestanden nur, soweit die eingesetzten PCs miteinander vernetzt waren. Eine Passwortänderung erfolgte teilweise nur ca. jedes halbe Jahr. Ob überhaupt eine Passwortänderung vorgenommen wurde, konnte im Landratsamt nicht überwacht werden.

Ich habe angeregt, in allen Bereichen des Landratsamtes, auch dort, wo noch keine vernetzten PCs eingesetzt wurden, dafür zu sorgen, dass eine Passwortänderung nach spätestens 90 Tagen systemtechnisch erzwungen wird. Ich verweise hierzu auch auf die Orientierungshilfe des Referates Technik und Organisation beim Bayerischen Landesbeauftragten für den Datenschutz, die Hinweise zur Passwortvergabe, -wahl und -verwaltung enthält, abrufbar unter www.datenschutz-bayern.de/inhalte/technik.htm.

8.1.3 Führung einer Bußgeldliste im Rahmen des Vollzugs der Gewerbeordnung

Das Landratsamt führte eine Bußgeldliste, in die die im Bereich des Gewerberechts verhängten Bußgelder eingetragen wurden. Mit dem Bayerischen Staatsministerium für Wirtschaft, Verkehr und Technologie bin ich der Auffassung, dass eine Ordnungswidrigkeitendatei im Bereich des Gewerberechts nicht erforderlich ist, da Geldbußen über DM 200 gem. § 149 Abs. 2 Satz 1 Nr. 3 GewO im Gewerbezentralregister eingetragen werden. Auf diese Weise können Behörden wiederholte Verstöße gegen gewerberechtliche Bestimmungen feststellen und ggf. bei der Zumessung der Geldbuße berücksichtigen. Auch das Führen einer Datei über Ordnungswidrigkeiten, für die Bußgelder unter DM 200 verhängt werden, ist nicht erforderlich, da der Gesetzgeber mit der Bestimmung des § 149 Abs. 2 Satz 1 Nr. 3 GewO insoweit eine abschließende Regelung getroffen hat.

8.2 Änderung der Landeswahlordnung

Am 1. Januar 2000 ist die Verordnung zur Änderung der Landeswahlordnung in Kraft getreten. Dabei konnte ich erreichen, dass die Daten der Stimmberechtigten, für die eine Auskunftssperre nach Art. 34 Abs. 5 des Meldegesetzes besteht, einschließlich der dazugehörenden fortlaufenden Nummer von der öffentlichen Auslegung des Wählerverzeichnisses ausgenommen werden und auf die Veröffentlichung des Tages der Geburt im Wählerverzeichnis verzichtet wird (§ 1 Nr. 3 der Verordnung, § 18 Abs. 2 der Landeswahlordnung). Die Landeswahlordnung wurde insoweit an die entsprechende Regelung in § 22 Abs. 2 der Gemeinde- und Landkreiswahlordnung angepasst.

Mein darüber hinausgehender Vorschlag, dass der Gesetzgeber auf die öffentliche Auslegung des Wählerverzeichnisses vollständig verzichten sollte, soll nach Mitteilung des Bayerischen Staatsministeriums des Innern im Rahmen der für diese Legislaturperiode vorgesehenen Novellierung der bundeswahlrechtlichen Vorschriften erneut geprüft werden.

Erreichen konnte ich außerdem, dass in den Eintragungslisten für Volksbegehren künftig auf die Angabe des Geburtsdatums verzichtet wird (§ 1 Nrn. 21 und 33 der Verordnung, § 78 Abs. 1 Satz 2 und Anlage 20 der Landeswahlordnung). Meiner Anregung im 18. Tätigkeitsbericht 1998 unter Nr. 8.3 wurde damit entsprochen.

8.3 Änderung des Gemeinde- und Landkreiswahlgesetzes

Im 18. Tätigkeitsbericht habe ich unter Nr. 8.2 darauf hingewiesen, dass nach Art. 4 Abs. 3 des Gemeinde- und Landkreiswahlgesetzes (GLKrWG) die Wahlausschüsse und die Wahlvorstände in öffentlicher Sitzung verhandeln, beraten und entscheiden. Das Gesetz sah auch bei einem Vorliegen schutzwürdiger Interessen einzelner Personen keine Behandlung in nichtöffentlicher Sitzung vor. Einem mir von der Presse vorgetragenen Fall, in dem eine Stadt unter Hinweis auf Art. 4 Abs. 3 GLKrWG den Gesundheitszustand eines für den Stadtrat vorgesehenen Nachrükkers unzulässig in öffentlicher Sitzung behandelt hat, habe ich zum Anlass genommen anzuregen, Art. 4 Abs. 3 GLKrWG dahingehend zu ergänzen, dass die Sitzungen der Wahlausschüsse und der Wahlvorstände nichtöffentlich sind, soweit das Wohl der Allgemeinheit oder berechtigte Ansprüche Einzelner dies erfordern. Mit der Neufassung von Art. 4 Abs. 4 des am 1. Januar 2000 in Kraft getretenen Gesetzes zur Änderung des Gemeinde- und Landkreiswahlgesetzes und anderer kommunalrechtlicher Vorschriften wurde meiner Forderung durch den Erlass einer Art. 52 Abs. 2 der Gemeindeordnung und Art. 46 Abs. 2 der Landkreisordnung entsprechenden Regelung entsprochen.

8.4 Virtueller Marktplatz

Die Bayerische Staatsregierung ist derzeit dabei, einen bayernweiten zentralen virtuellen Marktplatz zu errichten. Ziel des virtuellen Marktplatzes soll es sein, ein Abbild eines realen Marktplatzes mit Online-Techniken zu realisieren. Dadurch soll die Internetnutzung durch die Bürger und Unternehmen in Bayern weiter gesteigert werden.

Nach den Vorstellungen der Staatsregierung sollen außerdem auf der Ebene der Landkreise und der kreisfreien Städte dezentrale virtuelle Marktplätze errichtet werden. Betreiber des zentralen Marktplatzes und der dezentralen Marktplätze sollen private Stellen sein. Die dezentralen Marktplätze sollen in den bayernweiten Marktplatz integriert werden.

Auf den virtuellen Marktplätzen sollen eine Vielzahl von kommerziellen und nicht-kommerziellen „Warendienstleistungen und Informationen aller Art“ angeboten werden. Insbesondere soll auch ein Behördenwegweiser nach Vorgaben des Bayerischen Staatsministeriums des Innern angeboten werden. Ziel ist es, mit Hilfe eines Internet-Angebotes eine umfassende Information über alle von den staatlichen und – soweit beteiligt – kommunalen Behörden angebotenen Produkte und Leistungen zu schaffen (Behördenwegweiser). Dazu sollen u.a. Ansprechpartner, Telefonnummern, Zimmernummern, Öffnungszeiten etc. in das Internet eingestellt werden. Außerdem soll die Möglichkeit geschaffen werden, Antragsformulare online abzurufen, auszufüllen, auszudrucken und zu versenden. Des Weiteren soll der Behördenwegweiser so gestaltet werden, dass seitens der jeweiligen Behörden ein Work-Flow-System zur Vorgangsbearbeitung angeschlossen werden kann.

Aus dem Nebeneinander von zentralem virtuellen Marktplatz, dezentralen Marktplätzen, öffentlichen und privaten Anbietern sowie privaten Betreibern ergeben sich aus datenschutzrechtlicher Sicht eine Vielzahl rechtlicher und technisch-organisatorischer Fragen sowie Anforderungen, die ich der Bayerischen Staatskanzlei Anfang dieses Jahres in einem umfassenden Schreiben mitgeteilt habe. So bedürfen z. B. folgende Punkte einer Klärung und verbindlichen Festlegung:

- Zuständigkeiten und Verantwortlichkeiten (z. B. wer ist die speichernde Stelle und damit für den Inhalt des Angebots verantwortlich? Wie wird eine unzulässige Vermengung oder Ver-

knüpfung privater und behördlicher Inhalte vermieden? Für den Benutzer muss klar erkennbar sein, welchem Bereich der jeweilige Inhalt zuzuordnen ist).

- Nach dem Ausschreibungskonzept der Bayerischen Staatskanzlei soll der Marktplatz „zwar öffentlich-rechtliche Funktionen wahrnehmen, aber privat-wirtschaftlich betrieben werden". Es ist unklar, was damit gemeint ist.

- Wie erfolgt die Kommunikation zwischen Bürger und Verwaltung? Werden z. B. ausgefüllte Formulare direkt vom Bürger an die zuständige öffentliche Stelle gesandt oder erfolgt der Versand mit evtl. Zwischenspeicherung über den Betreiber des virtuellen Marktplatzes?

- Wie wird sichergestellt, dass keine unzulässigen Datenerhebungen- und nutzungen durch Dritte sowie Datenübermittlungen an Dritte und keine Anfertigung von Benutzerprofilen erfolgt?

- Wie wird die Vertraulichkeit, Integrität und Zuordenbarkeit der Datenübertragung gewährleistet?

- Wie werden die Vorschriften des Teledienstedatenschutzgesetzes – TDDSG – beachtet? Das Ausschreibungskonzept fordert an mehreren Stellen ein personalisiertes Angebot. In welcher Form erfolgt die Personalisierung? Welche personenbezogenen Aufzeichnungen benötigt der Betreiber des virtuellen Marktplatzes bezüglich der Abfragen?

Diese und zahlreiche weitere Fragen in meinen Schreiben an die Staatskanzlei wurden bis zur Übermittlung des Vorabdrucks dieses Berichts an den Beirat zur Vorberatung gem. Art. 30 Abs. 5 Satz 3 BayDSG nicht abschließend beantwortet. Auch das von mir mehrmals angeforderte Projektkonzept, das die Beurteilung datenschutzrechtlicher Fragen ermöglicht hätte, lag mir bis zu diesem Zeitpunkt nicht vor. Eine datenschutzrechtliche Bewertung des Projekts war mir deshalb bis dahin nicht möglich. Ich konnte mir somit noch kein eigenes Bild davon machen, ob bei dem Angebot „Virtueller Marktplatz" der Schutz der personenbezogenen Daten gewährleistet ist. Inzwischen ist ein Schreiben der Staatskanzlei vom 1.12. 2000 eingegangen. Zu dessen Inhalt verweise ich auf meine Ausführungen unter Nr. 1.1.2. Zusammengefasst führt die Staatskanzlei

darin aus, dass in einer ersten Ausbaustufe behördlicherseits lediglich Informationsangebote gemacht würden und die IP-Nummer des Nutzers nicht gespeichert würde. Eine abschließende Prüfung dieser Stellungnahme muß ich mir vorbehalten.

8.5 Serviceorientierte Verwaltung

Im Auftrag der Datenschutzkonferenz hat sich eine Arbeitsgruppe, an der ich teilgenommen habe, unter dem Vorsitz der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen mit Fragen der Modernisierung der Verwaltung und ihren technischen Aspekten beschäftigt. Ein Schwerpunkt der Tätigkeit der Arbeitsgruppe war die zunehmende Nutzung des Internets durch Behörden für Informationsangebote und zur Kommunikation mit dem Bürger. Ihre Ergebnisse hat die Arbeitsgruppe in einer Ausarbeitung unter dem Titel „Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ zusammengefasst. In dem Papier werden folgende Themen behandelt: Multifunktionaler Service (Bürgeramt, Bürgerbüro, Bürgerladen und Kundencenter), Call-Center, Informationsangebote öffentlicher Stellen im Internet, interaktive Verwaltung, Bürgerkarte, elektronische Auskunft, Akteneinsicht und Bürgerbeteiligung sowie Auslagerung von Verwaltungsfunktionen. Das Dokument wird voraussichtlich bis Ende des Jahres als Broschüre und im Internet veröffentlicht.

Zum Thema **Bürgerbüro** möchte ich dabei ergänzend und zusammenfassend insbesondere auf Folgendes hinweisen:

Das Konzept des Bürgerbüros besteht darin, dem Bürger eine einheitliche Anlaufstelle für die verschiedensten Anliegen anzubieten, so dass er sich den oft zeitraubenden Weg von einem Amt zum anderen sparen kann. Gleichzeitig soll dadurch auch der Publikumsverkehr in den Fachabteilungen verringert werden.

Die Aufgaben der Bürgerbüros sind nicht einheitlich definiert. Sie können über die Bereitstellung von Formularen, zentrale Anlaufstelle und Vermittlung bei Anfragen hinaus auch die Nutzung der unterschiedlichen IT-Verfahren und Datenbestände (z. B. Meldewesen, Steuerwesen, Abfallbeseitigung) sowie die Befugnisse der Beratung, Entgegennahme und Vorprüfung von Anträgen der verschiedensten Zuständigkeitsbereiche umfassen.
Bürgerbüros können somit dem Bürger in seinem Umgang mit der Verwaltung erhebliche Vorteile bieten und sind deshalb grundsätzlich auch aus der Sicht des Datenschutzes zu begrüßen. Die Zusammenfassung von Aufgaben aus verschiedenen Bereichen wirft allerdings datenschutzrechtliche Fragen auf.

So ist bei der Zusammenführung von unterschiedlichen Aufgabenstellungen und der Verarbeitung unterschiedlicher Datenbestände auf einem Arbeitsplatz die Feststellung des Bundesverfassungsgerichts in seinem Beschluss vom 18. Dezember 1987 (NJW 1988, 959), dass der Grundsatz der „informationellen Gewaltenteilung“ auch innerhalb der Gemeindeverwaltung gilt, zu berücksichtigen. Zwar gehört die Organisationshoheit der Gemeinden zum Kernbereich des Selbstverwaltungsrechts. Ihrer Gestaltungsfreiheit sind jedoch, wie das Bundesverfassungsgericht festgestellt hat, Grenzen gesetzt. Aus der Einheit der Gemeindeverwaltung folgt keine informationelle Einheit.

Diese vom Bundesverfassungsgericht verlangte „informationelle Gewaltenteilung“ in der Gemeindeverwaltung ist für den Bereich der Sozialleistungen im Gesetz ausdrücklich vorgeschrieben : Nach § 67 Abs. 9 S. 3 SGB X ist innerhalb einer Gebietskörperschaft jede für einen Sozialleistungsbereich zuständige Organisationseinheit eine (eigene) speichernde Stelle. Auch andere Organisationseinheiten **in derselben Kommune** dürfen Sozialdaten also nur zur Kenntnis erhalten, soweit Übermittlungsbefugnisse nach dem SGB einschlägig sind.

Bei der Einrichtung von Bürgerbüros muss dementsprechend darauf geachtet werden, dass nicht gegen das Sozialgeheimnis verstoßen wird. Solche Verstöße könnten sich etwa dadurch ergeben, dass Mitarbeiter im Bürgerbüro Zugriffs- und Kenntnisnahmemöglichkeiten betreffend Sozialdaten erhalten, die mit der Zweckbindung der für einen Sozialleistungsbereich bestimmten personenbezogenen Daten nicht zu vereinbaren sind. Zur Reduzierung des Risikos von Verletzungen des Sozialgeheimnisses im Bürgerbüro empfehle ich dringend, die Bearbeitung von Sozialleistungsangelegenheiten **nicht ausschließlich** im Bürgerbüro, sondern dort **nur zusätzlich** anzubieten, so dass dem Bürger die Möglichkeit verbleibt, sein Anliegen unmittelbar im zuständigen Sachgebiet vorzutragen. Auf diese Alternative ist im Bürgerbüro ausdrücklich hinzuweisen.

Außerdem sind bei der Ausgestaltung von Bürgerbüros die erforderlichen technisch-organisatorischen Maßnahmen zu treffen (z. B. ausreichende Abstände zwischen den einzelnen Arbeitsplätzen, um ein Mithören Dritter auszuschließen und die Möglichkeit für den Bürger, seine Angelegenheit in einem separaten Raum im Bürgerbüro vortragen zu können).

Bei der Prüfung eines Bürgerbüros sind diese Grundsätze im großen und ganzen beachtet worden.

8.6 Datenschutz bei Bürgerbegehren

8.6.1 Verlesen der Unterschriftenlisten in öffentlicher Gemeinderatssitzung

Bürger haben sich bei mir darüber beschwert, dass der erste Bürgermeister ihrer Gemeinde im Rahmen einer öffentlichen Gemeinderatssitzung die Vornamen, Familiennamen und Straßenangaben der Personen, die ein Bürgerbegehren gegen die Errichtung einer Anlage in der Gemeinde unterstützt hatten, verlesen hatte. Der erste Bürgermeister hatte auf diese Weise dem Gemeinderat demonstrieren wollen, dass das Bürgerbegehren nicht ausschließlich von Personen unterstützt wurde, die in der Nähe der geplanten Anlage wohnen, sondern dass Bürger aus dem gesamten Gemeindegebiet unterschrieben hatten.

Er war der Meinung, das Verlesen der Namen unterliege nicht der Geheimhaltung, da der sich jeweils als letzter eintragende Unterstützer Einsicht in die gesamte Namensliste nehmen könne. Außerdem vertrat er die Auffassung, dass nach Art. 18 a der Gemeindeordnung (GO) das Bürgerbegehren zwingend in öffentlicher Sitzung zu behandeln sei, weshalb es in seiner Gesamtheit als öffentlich anzusehen sei. Aus diesem Grund seien auch die unterstützenden Unterschriften öffentlich.

Ich habe den Vorgang datenschutzrechtlich wie folgt bewertet:

- **Sobald die Unterschriftslisten bei der Gemeinde abgegeben worden sind, unterliegen sie den datenschutzrechtlichen Bestimmungen**

Art. 18 a GO enthält keine Regelung über das Sammeln der Unterschriften. Dieses erfolgt nach der gängigen Praxis im Privatbereich. Die dabei erhobenen Daten unterliegen bis zu dem Zeitpunkt, in dem die Listen der Gemeinde übergeben werden, nicht den Bestimmungen des Bayerischen Datenschutzgesetzes (BayDSG) und nur unter eingeschränkten Voraussetzungen den Vorschriften des Bundesdatenschutzgesetzes. Nach geltendem Recht kann es daher nicht verhindert

werden, dass Unterzeichner und Dritte bis zur Übergabe der Listen an die Gemeinde Einsicht in diese nehmen.

Sobald die Unterschriftenlisten allerdings bei der Gemeinde abgegeben worden sind, unterliegen sie den einschlägigen gesetzlichen Bestimmungen. Sie dürfen daher nur unter den Voraussetzungen der Art. 15 ff BayDSG verarbeitet oder genutzt werden. Die Bekanntgabe und Auswertung von Daten in Unterschriftenlisten (auch auszugsweise) ist danach nur zulässig, wenn die Betroffenen darin eingewilligt haben oder eine Rechtsvorschrift dies erlaubt oder anordnet (Art. 15 Abs. 1 BayDSG).

- **Der Gemeinderat kann im Rahmen seiner Überwachungsbefugnis nach Art. 30 Abs. 3 GO die Einsichtnahme in die ausgewerteten Unterschriftslisten verlangen. Die Einsichtnahme hat unter Beachtung des Grundsatzes der Zweckbindung entweder in nichtöffentlicher Sitzung oder durch ein vom Gemeinderat durch Beschluss mit dieser Aufgabe beauftragtes Gemeinderatsmitglied in den Amtsräumen der Verwaltung zu erfolgen**

Da eine Einwilligung der Unterstützer des Bürgerbegehrens nicht vorlag, war für das Verlesen der Eintragungen in den Unterschriftenlisten eine Rechtsgrundlage erforderlich. Die **Bekanntgabe der Namen und Anschriften gegenüber den Gemeinderatsmitgliedern** stellt eine Nutzung personenbezogener Daten dar. Ihre Zulässigkeit richtet sich mangels einer spezialgesetzlichen Regelung nach Art. 17 Abs. 1 BayDSG. Danach durften die Daten an den Gemeinderat weitergegeben werden, soweit dies u.a. zur Aufgabenerfüllung dieses Gremiums erforderlich war.

Nach Art. 18 a Abs. 8 Satz 1 GO entscheidet der Gemeinderat über die Zulässigkeit eines Bürgerbegehrens. Er hat in diesem Zusammenhang u.a. zu prüfen, ob das Bürgerbegehren von einer ausreichenden Zahl stimmberechtigter Gemeindebürger unterstützt wird (Art. 18 a Abs. 5 bis 7 GO). Die Entscheidung des Gemeinderats beruht dabei auf entsprechenden Informationen des ersten Bürgermeisters. Dieser bzw. die Gemeindeverwaltung wertet die Unterschriftenlisten dahingehend aus, wieviel antragsberechtigte Gemeindebürger unterschrieben haben sowie ob die Eintragungen gültig oder ungültig sind und trägt dem Gemeinderat das Ergebnis vor.

Dem Gemeinderat bleibt es dabei unbenommen, im Rahmen seiner Überwachungsbefugnis nach Art. 30 Abs. 3 GO die Einsichtnahme in die ausgewerteten Unterschriftenlisten zu verlangen. Wegen des Grundsatzes der Zweckbindung (Art. 17 Abs. 1 Nr. 2 BayDSG) darf aber auch der Gemeinderat die Unterschriftenlisten nur hinsichtlich der Frage einsehen, ob das Bürgerbegehren von einer ausreichenden Zahl antragsberechtigter Gemeindebürger unterschrieben worden ist und ob die Gemeindeverwaltung die Eintragungen in zutreffender Weise als gültig oder ungültig eingestuft hat (vgl. auch Thum, Kommunalpraxis 1997, S. 379, 381, 382).

Im vorliegenden Fall hat der erste Bürgermeister die Vornamen, Familiennamen und die Anschriften der Personen, die sich in die Unterschriftenlisten für das Bürgerbegehren eingetragen haben, in öffentlicher Gemeinderatssitzung verlesen, um dem Gemeinderat zu demonstrieren, dass das Bürgerbegehren nicht ausschließlich von Personen unterstützt wird, die in der Nähe der geplanten Anlage wohnen, sondern dass Bürger aus dem gesamten Gemeindegebiet unterschrieben haben. Die Datenweitergabe an den Gemeinderat erfolgte somit nicht auf dessen Verlangen hin zum Zwecke der Ausübung der Überwachungsbefugnis nach Art. 30 Abs. 3 GO. Sie war also zur Aufgabenerfüllung des Gemeinderats nicht erforderlich und damit bereits aus diesem Grunde unzulässig. Hinzu kommt, dass eine Einsichtnahme in die Unterschriftenlisten durch den Gemeinderat im Vollzug des Art. 30 Abs. 3 GO mit Rücksicht auf die schutzwürdigen Belange der betroffenen Bürger nicht in der Öffentlichkeit erfolgen darf, sondern in nichtöffentlicher Sitzung bzw. durch ein vom Gemeinderat durch Beschluss mit dieser Aufgabe beauftragtes Gemeinderatsmitglied in den Amtsräumen der Verwaltung zu erfolgen hat (siehe dazu auch weiter unten).

- **Das Verlesen der Unterschriftenlisten in öffentlicher Gemeinderatssitzung ist eine unzulässige Datenübermittlung an die Öffentlichkeit**

Das Verlesen der Unterschriftenlisten in öffentlicher Gemeinderatssitzung war nicht nur eine Datenweitergabe an die Gemeinderatsmitglieder, sondern gleichzeitig auch eine **Datenübermittlung an die anwesenden Zuhörer und Pressevertreter.** Diese war nicht nach Art. 18 a GO zulässig. Diese Vorschrift regelt nicht, ob die Behandlung des Bürgerbegehrens bzw. die Entscheidung über dessen Zulässigkeit in öffentlicher oder nichtöffentlicher Sitzung zu erfolgen hat. Dies ergibt sich vielmehr aus Art. 52 Abs. 2 GO. Danach sind die Sitzungen des Gemeinderats

öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche Einzelner entgegenstehen.

Die Beratung und Abstimmung über die Zulässigkeit des Bürgerbegehrens in öffentlicher Gemeinderatssitzung ist regelmäßig dann unproblematisch, wenn zur Frage, ob das Bürgerbegehren von einer ausreichenden Zahl stimmberechtigter Gemeindebürger unterstützt wird, lediglich das **Ergebnis** der Überprüfung der Unterschriftenlisten bekanntgegeben wird. Der namentlichen Erwähnung der Unterstützer des Bürgerbegehrens in öffentlicher Gemeinderatssitzung stehen dagegen berechtigte Ansprüche der Betroffenen entgegen. Diese müssen darauf vertrauen können, dass ihre Daten entsprechend den einschlägigen gesetzlichen Bestimmungen behandelt werden und im Bereich der Verwaltung und des zuständigen Entscheidungsgremiums verbleiben. Wie bereits ausgeführt, unterliegen auch die im Privatbereich gesammelten Unterschriften den einschlägigen gesetzlichen Bestimmungen, sobald sie bei der Gemeinde abgegeben worden sind.

Abgesehen davon habe ich zu dem Vorhalt, die Daten seien nicht schutzwürdig, weil der sich als zuletzt eintragende Unterstützer die ganze Namensliste zur Kenntnis nehmen könne, auf Folgendes hingewiesen:

Nach dem allgemein praktizierten Verfahren der Unterschriftsleistung kann zwar angenommen werden, dass Unterschriftsleistende die Kenntnis ihrer Eintragung durch Nacheintragende auf der laufenden Unterschriftenliste zwangsläufig akzeptieren. Es kann jedoch nicht angenommen werden, dass sie auch davon ausgehen, geschweige damit einverstanden sind, dass die Gemeinde, an die sich das mit der Unterschriftenaktion verfolgte Begehren richtet, die Unterschriftenliste einzelnen Dritten oder gar der Öffentlichkeit bekannt gibt. Es ist auch ein erheblicher Unterschied, ob Personen bei der Eintragung von Voreintragungen Gleichgesinnter Kenntnis nehmen können oder ob die Unterschriftenliste Dritten oder gar der Allgemeinheit mitgeteilt wird.
Die Bekanntgabe der Familiennamen, Vornamen und Anschriften der Unterstützer des Bürgerbegehrens in öffentlicher Gemeinderatssitzung gegenüber der Öffentlichkeit war somit ebenfalls unzulässig. Wie bereits ausgeführt, kommt neben der Auswertung der Unterschriftenlisten durch den ersten Bürgermeister bzw. die Gemeindeverwaltung zur Feststellung, ob die Voraussetzungen des Art. 18 a Abs. 5 bis 7 GO vorliegen, nur eine Einsichtnahme in die Listen durch den

Gemeinderat bzw. ein von diesem beauftragtes Gemeinderatsmitglied im Vollzug des Art. 30 Abs. 3 GO in nicht-öffentlicher Sitzung oder in den Amtsräumen in Betracht.

- **Die Unterschriftenlisten dürfen nur hinsichtlich der Frage ausgewertet werden, ob das Bürgerbegehren von einer ausreichenden Zahl stimmberechtigter Gemeindebürger unterschrieben worden ist**

Ein weiterer datenschutzrechtlicher Verstoß liegt in der **Auswertung der Unterschriftenlisten nach der Nähe der Unterzeichner zum Gegenstand des Bürgerbegehrens**. Der erste Bürgermeister teilte dazu mit, er habe die Namen und Anschriften der Unterstützer verlesen, um dem Gemeinderat zu demonstrieren, dass es sich nicht ausschließlich um in der Nähe der geplanten Anlage wohnende Bürger handelt, sondern dass das Begehren von quer im Gemeindegebiet beheimateten Personen unterstützt worden sei. Er hat damit den Grundsatz der Zweckbindung (Art. 17 Abs. 1 Nr. 2 BayDSG) nicht beachtet. Die Unterschriften dürfen nur hinsichtlich der Frage ausgewertet werden, ob das Bürgerbegehren von einer ausreichenden Zahl stimmberechtigter Gemeindebürger unterschrieben worden ist.

- **Das Verlesen der Unterschriftenlisten in öffentlicher Gemeinderatssitzung und ihre Auswertung nach der örtlichen Nähe der Unterzeichner zum Gegenstand des Bürgerbegehrens sind erhebliche Datenschutzverstöße, da sie geeignet sind, auf Unterzeichner des Bürgerbegehrens eine abschreckende Wirkung ausüben**

Ich habe das Verlesen der Familiennamen, Vornamen und Straßenangaben der das Bürgerbegehren unterstützenden Personen in öffentlicher Gemeinderatssitzung und die Auswertung der Unterschriftenlisten nach der örtlichen Nähe der Unterzeichner zum Gegenstand des Bürgerbegehrens nach Art. 31 Abs. 1 BayDSG beanstandet. Von der Beanstandung konnte ich nicht absehen, weil es sich nicht um unerhebliche Datenschutzverstöße gehandelt hat. Das öffentliche Verlesen der Namen und Anschriften der Unterstützer und die Auswertung der Unterschriftenlisten nach der Nähe der Unterzeichner zum Gegenstand des Bürgerbegehrens sind geeignet, auf Unterzeichner des Bürgerbegehrens eine abschreckende Wirkung auszuüben und sie davon abzuhalten, sich künftig nochmals an dem gesetzlich ausdrücklich vorgesehenen Rechtsinstitut des Bürgerbegehrens zu beteiligen.

In diesem Zusammenhang weise ich außerdem darauf hin, dass sowohl das Innenministerium als auch ich selbst in der Vergangenheit immer wieder darüber aufgeklärt haben, dass die Unterschriftenlisten von Bürgerbegehren nur zu dem Zweck ausgewertet werden dürfen, ob eine ausreichende Zahl stimmberechtigter Gemeindebürger unterschrieben hat (Rundschreiben des Innenministeriums vom 06.03.1996, 17. Tätigkeitsbericht 1995/1996 Nr. 8.4.2 und 18. Tätigkeitsbericht 1997/1998 Nr. 8.4.2). In meinem 18. Tätigkeitsbericht habe ich mich außerdem zur unzulässigen Einsichtnahme von Dritten in Unterschriftenlisten für Bürgerbegehren geäußert. Die Unzulässigkeit der öffentlichen Bekanntgabe der Namen und Adressen in den Unterstützerlisten und die Auswertung der Listen nach der örtlichen Nähe der Unterzeichner zu dem Gegenstand des Bürgerbegehrens hätte daher bekannt sein müssen.

8.6.2 Nutzung von Unterschriftenlisten zur Gewinnung von Wahlhelfern

Von der Presse und aus der Bevölkerung bin ich auf folgenden Sachverhalt aufmerksam gemacht worden:
Im Rahmen eines Bürgerbegehrens nach Art. 12 a LKrO hatte ein Landratsamt den Landkreisgemeinden die Namen der Bürger, die unter einer Anschrift der jeweiligen Gemeinde das Bürgerbegehren unterstützt haben, zur Überprüfung der Unterschriftsberechtigung mitgeteilt. Eine Gemeinde berief daraufhin einige dieser Bürger zu Wahlvorstandsmitgliedern für den Bürgerentscheid in dem Verfahren. Die Berufung erfolgte mit einem ausdrücklichen Hinweis auf die Unterstützung des Bürgerbegehrens. In den Berufungsschreiben der Gemeinde an die Betroffenen heißt es wörtlich: „Da Sie Ihr Interesse am Bürgerbegehren bekundet haben, setzen wir Ihre Bereitschaft voraus, auch am Bürgerentscheid aktiv teilzunehmen.“

Ich habe den Vorgang datenschutzrechtlich wie folgt bewertet.

Der Gemeinde sind die Namen und Anschriften der Bürger dieser Gemeinde, die das Bürgerbegehren unterstützt haben, vom Landratsamt zur Überprüfung der Unterschriftsberechtigung nach Art. 12 a Abs. 5 LKrO übermittelt worden. Da die Betroffenen in eine Verwendung ihrer Daten zur Berufung als Wahlvorstandsmitglieder nicht eingewilligt hatten und auch kein Fall einer zulässigen Zweckänderung vorliegt, hätten die übermittelten Daten nur zu dem genannten Zweck (Überprüfung der Unterschriftsberechtigung) genutzt werden dürfen.

Eine Zweckänderung zur Gewinnung ehrenamtlicher Wahlhelfer ist nach Art. 17 Abs. 2 Nr. 12 des Bayerischen Datenschutzgesetzes (BayDSG) nur bei den in dieser Vorschrift abschließend aufgeführten Beschäftigtendaten von Angehörigen des öffentlichen Dienstes zulässig. Art. 17 Abs. 2 Nr. 12 BayDSG ist eine bereichsspezifische, die Wahlorganisation betreffende Regelung aus dem Bereich des Wahlrechts. Sie wurde geschaffen, um die in der Praxis außerordentlich weit verbreitete Besetzung der Wahlvorstände mit Angehörigen des öffentlichen Dienstes nicht zu gefährden (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, Art. 17 Rdnr. 45 und 45 a). Aus der abschließenden Regelung des Art. 17 Abs. 2 Nr. 12 BayDSG („und sich auf die Weitergabe oder Übermittlung ... beschränkt“) ergibt sich, dass eine Nutzung anderer als der in dieser Vorschrift genannten Daten zur Gewinnung von Wahlhelfern unzulässig ist.

Mit der Verwendung der vom Landratsamt für die Prüfung der Unterschriftenberechtigung übermittelten Daten für die Berufung zum Wahlvorstandsmitglied verstieß die Gemeinde damit gegen den Grundsatz der Zweckbindung in Art. 17 Abs. 1 Nr. 2 BayDSG. Ich habe diesen Datenschutzverstoß nach Art. 31 Abs. 1 BayDSG beanstandet.

Ein Absehen von der Beanstandung nach Art. 31 Abs. 3 BayDSG war mir nicht möglich, weil es sich nicht um einen unerheblichen Datenschutzverstoß handelte. Zwar ist die Berufung zum Wahlvorstandsmitglied ein Ehrenamt, zu dem jede wahlberechtigte Person verpflichtet ist. Mit der Berufung zu diesem Ehrenamt ist objektiv auch keine Benachteiligung für die betroffenen Bürger verbunden. Die gesetzlich unzulässige Verknüpfung der Unterstützung eines Bürgerbegehrens mit der Einteilung zum Wahlhelfer, verbunden mit einem ausdrücklichen Hinweis an die Betroffenen, dass ihre Berufung zum Wahlhelfer auf ihre Teilnahme am Bürgerbegehren zurückzuführen ist, kann von Unterzeichnern des Bürgerbegehrens jedoch als nachteilige Folge ihrer Teilnahme am Bürgerbegehren verstanden werden und ist geeignet, sie davon abzuhalten, sich künftig nochmals an dem gesetzlich ausdrücklich vorgesehenen Rechtsinstitut des Bürgerbegehrens zu beteiligen.

8.7 Führung zentraler Adressdateien

Von mehreren Kommunen wurde ich mit folgendem Fall befasst: Die Kommunen führen jeweils für ihre gesamte Verwaltung eine automatisierte zentrale Adressdatei für alle Zahlungspflichtigen bzw. –empfänger, in der neben dem Namen und der Adresse auch die Bankverbindung sowie teilweise weitere Merkmale, wie für Zwecke der Erhebung der Grundsteuer benötigte Objektdaten, gespeichert werden. Sobald über einen Suchbegriff aus der Datei eine Adresse abgerufen werden soll, werden, ohne dass zu diesem Zeitpunkt eine Einzelfallbearbeitung stattfindet, allgemein auch die Bankverbindung und, in einem von mir zu beurteilenden Fall, auch weitere Objektdaten am Bildschirm angezeigt. Ich habe den Gemeinden Folgendes mitgeteilt:

Der Online-Abruf aus der Adressdatei stellt eine Nutzung der darin gespeicherten personenbezogenen Daten dar. Sie ist nur dann zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet, oder wenn der Betroffene darin eingewilligt hat (Art. 15 Abs. 1 BayDSG). Da eine, auch mutmaßliche, Einwilligung i.d.R. nicht vorliegen wird, dürfen die Daten nur genutzt werden, wenn eine Rechtsgrundlage dafür vorhanden ist.

Soweit die Verwendung der Daten in spezialgesetzlichen Bestimmungen geregelt ist (z.B. SGB X, BayBG, AO) ist zu prüfen, ob diese Vorschriften einen Abruf durch den im Schreiben der Gemeinde genannten Personenkreis zulassen.

Einer Eingabe konnte ich entnehmen, dass es im Rahmen einer derartigen Adressdatei einer Stadt für alle Anordnungsdienststellen u.a. möglich war, Daten über Immobilienobjekte sowohl von Bürgern als auch von städtischen Bediensteten einzusehen. Es war davon auszugehen, dass die genannten Informationen aus den beim Stadtsteueramt für Zwecke der Erhebung der Grundsteuer eingerichteten Datenbeständen stammten.

Ich habe darauf hingewiesen, dass in diesem Zusammenhang Bestimmungen der Abgabenordnung zu beachten sind, insbesondere § 30 AO (Steuergeheimnis). Eine Durchbrechnung des Steuergeheimnisses ist nur aufgrund der abschließenden Regelung des § 30 Abs. 4 AO zulässig. Für den in Rede stehenden Sachverhalt ist kein zulässiger Durchbrechungstatbestand gegeben. Insbesondere steht ein Zugriff auf Immobilienobjekte eines Bürgers durch Bedienstete der Stadt

außerhalb des Stadtsteueramts in der Regel nicht im Zusammenhang mit der Durchführung eines Verfahrens in Steuersachen (§ 30 Abs. 4 Nr. 1 AO). Auch § 31 Abs. 3 AO (i.V.m. § 30 Abs. 4 Nr. 2 AO) führt zu keinem anderen Ergebnis, da nach dieser Vorschrift ausschließlich Namen und Anschrift von Grundstückseigentümern für bestimmte andere im Gesetz genannte Zwecke genutzt werden dürfen und nicht auch Objektdaten. Die vorgenannten Bestimmungen gelten im übrigen auch für Merkmale aus der Gewerbesteuerveranlagung und auch für Daten aus der Erhebung von bestimmten anderen kommunalen Abgaben (Art. 13 Abs. 1 Nr. 1 c KAG). Letztendlich ist der Zugriff auf die dem Steuergeheimnis unterliegenden Merkmale ausnahmslos auf die jeweils zuständigen Mitarbeiter im Stadtsteueramt zu beschränken.

Ich habe deshalb gebeten, das Verfahren datenschutzgerecht zu modifizieren. Das Verfahren wurde inzwischen durch einen Zugriffsschutz erweitert. Der Zugriffsschutz ist über einen eigenen Dialogteil individuell vom Nutzer des Verfahrens einstellbar, so dass bei entsprechender Voreinstellung nur noch Mitarbeiter aus den jeweiligen Fachämtern (hier: Stadtsteueramt) auf die für sie freigegebenen Objektarten zugreifen können. Damit ist sichergestellt, dass in dem von mir zu beurteilenden Sachverhalt nur mehr befugte Personen i.S.d. § 30 AO auf die Objektdaten zugreifen können.

Mit dem Zugriff auf die Daten von Bediensteten der Kommune, soweit es sich um Personalaktendaten handelt (z.B. für die Überweisung der Reisekosten) und der Bedienstete nicht als Privatperson betroffen ist, war ich ebenfalls befasst. Ich bin dabei zu dem Ergebnis gekommen, dass ein (lesender) Zugriff aller Haushaltssachbearbeiter und Anordnungsbefugten nicht zulässig ist. Ich habe deshalb vorgeschlagen, die Daten der Bediensteten außerhalb der zentralen Adressdatei zu speichern bzw. einen (auch nur lesenden) Zugriff auf die Personalsachbearbeiter zu beschränken; dies wurde von den betroffenen Kommunen umgesetzt. Ergänzend verweise ich hierzu auch auf Art. 100 h Abs. 5 BayBG.

Soweit die Nutzung der Daten keinen spezialgesetzlichen Bestimmungen unterliegt, ist sie u.a. nur dann zulässig, wenn sie zur Aufgabenerfüllung der speichernden Stelle erforderlich ist (Art. 17 Abs. 1 Nr. 1 BayDSG). Dies ist hinsichtlich der Bankverbindung nicht der Fall, wenn der Sachbearbeiter im Zeitpunkt des Abrufs lediglich die aktuelle Anschrift des Zahlungspflich-

tigen bzw. –empfängers benötigt und feststeht, dass die Bankverbindung auch für die anschließende weitere Sachbearbeitung nicht erforderlich ist.

Im Übrigen setzt die Nutzung der Daten in der Adressdatei voraus, dass der Abruf für Zwecke erfolgt, für die die Daten erhoben bzw. gespeichert worden sind (Art. 17 Abs. 1 Nr. 2 BayDSG). Dies bedeutet, dass die Datensätze der Adressdatei, die der Stadt z. B. zur Rückzahlung zuviel bezahlter Abwassergebühren überlassen wurden, nicht zur Erfüllung sonstiger Aufgaben, z. B. für die Pfändung rückständiger Erschließungsbeiträge, verwendet werden dürfen, es sei denn, es liegen die Voraussetzungen des Art. 17 Abs. 2 bis 4 BayDSG vor.

Ein zusätzliches Problem ergibt sich bei den Personen, die städtischen Dienststellen zu deren jeweiliger Aufgabenerfüllung verschiedene Bankverbindungen zur Verfügung stellen. Die Nutzung einer vom Betroffenen dafür nicht vorgesehenen Bankverbindung durch eine städtische Dienststelle widerspricht nicht nur dessen Willen, sondern könnte für ihn mit weiteren Nachteilen verbunden sein (z.B. unerwünschte Kenntnisnahme durch den Ehegatten bei einer gemeinsamen Verfügungsbefugnis für dieses Konto).

Schließlich stellt sich die Frage, welche städtische Stelle bei einer zentralen Adressdatei als speichernde Stelle gilt und damit die Verantwortung für die Richtigkeit der Angaben trägt.

Ich habe vorgeschlagen, den Sachbearbeitern zur Ermittlung aktueller Adressen die Möglichkeit eines Online-Abrufs aus dem Einwohnermelderegister bzw. dem Gewerberegister einzuräumen, soweit dies zu ihrer Aufgabenerfüllung erforderlich ist (Art. 31 Abs. 7 i.V.m. Abs. 1 MeldeG, § 14 Abs. 7 i.V.m. Abs. 6 Satz 1 GewO). Auf diesem Weg wird die nicht erforderliche und zweckwidrige Kenntnisnahme der Bankverbindung vermieden.

8.8 Videoüberwachung öffentlicher Plätze durch Kommunen

Im Berichtszeitraum war ich mit der datenschutzrechtlichen Problematik einer Videoüberwachung öffentlicher Plätze durch Gemeinden befasst. Kommunen hatten sich an mich gewandt, die aus Gründen der Prävention, Gefahrenabwehr und Schadensverhütung eine Videoüberwachung öffentlicher Plätze, insbesondere des Marktplatzes, beabsichtigten.

Aus datenschutzrechtlicher Sicht vertrete ich dazu folgende Auffassung:

Die Beobachtung der Bürger als Passanten auf öffentlichen Plätzen durch den Einsatz von Videotechnik stellt einen Eingriff in deren allgemeines Persönlichkeitsrecht dar. Soweit im Rahmen der Videoüberwachung Personen z. B. durch Heranzoomen identifizierbar sind, liegt auch eine Erhebung personenbezogener Daten i. S. d. Art. 4 Abs. 1 des Bayerischen Datenschutzgesetzes (BayDSG) vor. Wird die Videokamera dabei nicht nur zur – räumlich versetzten – Überwachung über einen oder mehrere Bildschirme von zentraler Stelle aus eingesetzt, sondern werden Videoaufzeichnungen gefertigt, die im Nachhinein betrachtet und ausgewertet werden können, liegt auch eine Speicherung personenbezogener Daten vor. Das Speichern personenbezogener Daten ist eine Form der Datenverarbeitung (Art. 4 Abs. 6 Satz 1 BayDSG). Die nachträgliche Betrachtung und Auswertung der Videoaufzeichnungen ist eine Datennutzung im Sinn des Art. 4 Abs. 7 BayDSG.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ohne Rechtsgrundlage oder informierte Einwilligung der Betroffenen ist unzulässig (Art. 15 Abs. 1 BayDSG). Eine Einwilligung in die Datenerhebung, -verarbeitung und -nutzung ist bei einer Videoüberwachung öffentlicher Plätze schon angesichts eines nicht bestimmbaren Personenkreises potenziell Betroffener und der fehlenden Freiwilligkeit ausgeschlossen.

Eine bereichsspezifische Rechtsgrundlage für die Videoüberwachung öffentlicher Plätze durch Kommunen gibt es nicht. Die Videoüberwachung beurteilt sich deshalb nach Art. 16 BayDSG.

Gegen Übersichtsaufnahmen ohne Personenbezug von Plätzen mit Gefährdungspotenzial und zu tatrelevanten Zeiten habe ich als Einzelfall betrachtet übergangsweise keine Bedenken. Eine flä-

chendeckende Beobachtung mit Videokameras ohne diese örtliche und zeitliche Einschränkung halte ich aus verfassungsrechtlichen Gründen für unzulässig, weil eine derart umfassende Beobachtungsmöglichkeit den Bürger unter einen ständigen Anpassungsdruck setzen würde und damit gegen das Grundrecht aus Art. 1 und 2 des Grundgesetzes auf freie Entfaltung der Persönlichkeit verstoßen würde.

Das Heranzoomen von Personen und deren Aufzeichnung mit der Möglichkeit der Identifizierung halte ich im Fall einer konkreten Gefahr für die öffentliche Sicherheit und Ordnung für zulässig.

Nach Art. 16 Abs. 2 Satz 1 BayDSG sind personenbezogene Daten primär beim Betroffenen mit seiner Kenntnis zu erheben. Auf die Videoüberwachung ist deshalb durch Hinweisschilder aufmerksam zu machen. Aufzeichnungen sind zu löschen, sobald sie zur Feststellung von Betroffenen und zur Beweissicherung nicht mehr erforderlich sind.

Im Übrigen bin ich der Ansicht, dass im Hinblick auf die zunehmende Tendenz, öffentliche Plätze mit Videotechnik zu überwachen, und das Erfordernis einer landesweit einheitlichen Handhabung, der Gesetzgeber die Voraussetzungen und Grenzen einer Videoüberwachung öffentlicher Plätze klar definieren sollte. In einer gesetzlichen Regelung müssen eine strenge Zweckbindung, eine Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen, die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen, die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten und die Löschung zur Aufgabenerfüllung nicht mehr benötigter Daten binnen kurzer Fristen sichergestellt werden.
Ich habe die Aufnahme einer entsprechenden Regelung in die diesjährige Novelle des Bayerischen Datenschutzgesetzes gefordert. Das ist mit Hinweis auf die Eilbedürftigkeit der Vorlage (Umsetzung der EU-Datenschutzrichtlinie) leider nicht geschehen. Das Staatsministerium des Innern hat die Prüfung aber für eine zweite Novelle zugesagt. Ich halte meine Forderung aufrecht.

8.9 Information der Presse über Tagesordnungspunkte, die in öffentlicher Gemeinderatssitzung behandelt werden

Ein Bürger hat sich darüber beschwert, dass eine Stadt in einem Bauleitplanverfahren ein Abwägungsprotokoll zur Beschlussfassung in öffentlicher Stadtratssitzung an die Presse übermittelt hatte. In diesem Abwägungsprotokoll waren Schreiben des Petenten und weiterer Eingabeführer an die Stadt unter Angabe von Name und Adresse abgedruckt.

Ich habe den Vorgang datenschutzrechtlich wie folgt bewertet:

Das Abwägungsprotokoll war eine Sitzungsvorlage für die Beschlussfassung in der öffentlichen Stadtratssitzung. Sitzungsvorlagen der Verwaltung sind **interne** Ausarbeitungen für den Gemeinderat bzw. den Ausschuss. Die Vorlagen werden nur insoweit in die öffentliche Sitzung eingeführt, als sie der Bürgermeister mündlich vorträgt.
Will die Stadt die Presse über Tagesordnungspunkte, die in öffentlicher Stadtratssitzung behandelt werden, unterrichten, so hat sie in jedem Fall vorab 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. Die Weitergabe personenbezogener Daten an die Presse ist eine Datenübermittlung an nicht-öffentliche Stellen, die ohne Einwilligung der Betroffenen nach Art. 19 Abs. 1 Nr. 2 Bayer. Datenschutzgesetz (BayDSG) nur zulässig ist, wenn die Presse ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht, bzw. ein solches Interesse offenkundig ist, und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden (Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Handbuch XII. 3.).

Die Presse kann sich aus der Tagesordnung und in der öffentlichen Sitzung über das Anliegen informieren. Darüber hinaus kommt eine Information der Presse unter den Voraussetzungen des Art. 19 Abs. 1 Nr. 2 BayDSG, z.B. im vorliegenden Fall eine zusammenfassende Mitteilung, welche Einwendungen im Wesentlichen im Bebauungsplanverfahren erhoben wurden, in Betracht. Will die Stadt die Presse durch Übermittlung von Sitzungsvorlagen über Tagesordnungs-

punkte unterrichten, die in öffentlicher Stadtratssitzung behandelt werden, dann muss sie diese Sitzungsvorlagen durch Kürzen, Schwärzen etc. so abändern, dass sie nur noch Informationen enthalten, die ohne Bedenken der Öffentlichkeit zugänglich gemacht werden dürfen.

Durch die Weitergabe von Schreiben, die ein Bürger an die Gemeinde richtet, ohne dessen Einwilligung an die Presse, sei es in Ablichtung oder wie im vorliegenden Fall abgedruckt im Abwägungsprotokoll, werden regelmäßig schutzwürdige Interessen des betroffenen Bürgers beeinträchtigt. Der Bürger muss grundsätzlich darauf vertrauen können, dass mit seinem Anliegen nur die zuständigen Stellen befasst werden, das Schreiben also im internen Verhältnis Bürger-Verwaltung-Entscheidungsgremium verbleibt und jedenfalls nicht ohne besonderen Rechtsgrund durch Weiterleitung an die Presse der Öffentlichkeit zugänglich gemacht wird. Der Bürger muss es zwar hinnehmen, dass seine einzelnen Einwendungen der Sache nach im Gemeinde- bzw. Stadtrat öffentlich erörtert werden, soweit nicht eine Behandlung nach Art. 52 Abs. 2 der Gemeindeordnung in nichtöffentlicher Sitzung zu erfolgen hat. Er muss aber nicht damit rechnen, dass seine volle Adresse und seine Formulierungen im Einzelnen in vollem Umfang der Presse und damit der Öffentlichkeit zur Verfügung gestellt werden.

Die in der Übergabe des Abwägungsprotokolls liegende Übermittlung der Schreiben des Petenten und der weiteren Eingabeführer an die Presse stellte damit eine unzulässige Datenübermittlung dar.

Von einer förmlichen Beanstandung konnte ich gem. Art. 31 Abs. 3 BayDSG dieses Mal noch absehen, weil die Presse in ihrer Berichterstattung über die Behandlung des Bebauungsplanverfahrens im Stadtrat weder aus den Schreiben zitiert, noch die Eingabeführer namentlich erwähnt hat.

8.10 Weitergabe einer Unterschriftenliste und von Bürgereingaben in einem Bauleitplanverfahren an ein Privatunternehmen

Die Presse hat mir mitgeteilt, dass eine Gemeinde eine bei ihr gegen eine Baugebietsausweisung eingereichte Unterschriftenliste an ein Privatunternehmen weitergegeben hatte. Die von mir dazu befragte Gemeinde hat bestätigt, dass sich Bürger im Rahmen eines Bauleitplanverfahrens zur Änderung des Flächennutzungs- und Landschaftsplanes der Gemeinde und zur Aufstellung eines Bebauungsplanes in einem Schreiben gegen die geplante Ausweisung eines Industriegebiets ausgesprochen hatten.

Dem an die Gemeinde gerichteten Schreiben war eine Unterschriftenliste mit 99 Unterschriften beigefügt. Die Liste enthielt die Namen, die Anschriften und die Unterschriften der Unterzeichner.

Weiter hat die Gemeinde mitgeteilt, dass sie sämtliche Stellungnahmen, die während der Bürgerbeteiligung und der Beteiligung der Träger öffentlicher Belange bei ihr eingegangen sind, in Ablichtung an die „Vorhabensträgerin des Bauleitplanverfahrens“, eine Privatfirma, weitergegeben hat. Darunter sei auch das Schreiben mit der Unterschriftenliste gewesen. Die Weitergabe sei erfolgt, damit die vorgebrachten Anregungen bzw. Bedenken in öffentlicher Gemeinderatssitzung, unter Einbeziehung der Vorhabensträgerin, abgehandelt werden können. Nachdem Bauleitplanverfahren öffentlich abzuwickeln seien, seien keine personenbezogenen Daten in unzulässiger Weise weitergegeben worden.

Ich habe den Vorgang datenschutzrechtlich wie folgt bewertet:

Die Weitergabe des Schreibens und der Unterschriftenliste an die Firma war eine Übermittlung personenbezogener Daten an Dritte (Art. 4 Abs. 6 Nr. 3 a BayDSG). Personenbezogene Daten sind gem. Art. 4 Abs. 1 BayDSG Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene). Dazu gehören der Name, die Anschrift und die geleistete Unterschrift. Die Angaben in dem Schreiben und in der Unterschriftenliste stellen damit personenbezogene Daten im Sinn des Bayerischen Datenschutzgesetzes dar.

Mangels bereichsspezifischer Rechtsvorschriften beurteilte sich die Datenübermittlung im vorliegenden Fall nach Art. 19 Abs. 1 Nr. 2 BayDSG. Nach dieser Vorschrift ist die Übermittlung personenbezogener Daten an eine nicht-öffentliche Stelle u.a. nur dann zulässig, wenn diese ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt. Ein berechtigtes Interesse ist jedes nach vernünftigen Erwägungen gerechtfertigte Interesse wirtschaftlicher, rechtlicher oder ideeller Art. Im vorliegenden Fall hatte die Firma ein wirtschaftliches Interesse an der Ausweisung eines Industriegebiets. Sie hatte damit ein berechtigtes Interesse an der Kenntnis, dass gegen das Vorhaben eine Liste mit 99 Unterschriften in der Gemeinde eingereicht worden war und welche Gründe von den Unterzeichnern gegen das Vorhaben vorgetragen wurden. Ein darüber hinausgehendes berechtigtes Interesse an der Kenntnis von Namen und Anschriften der einzelnen Unterzeichner der Liste bestand nicht.

Art. 19 Abs. 1 Nr. 2 BayDSG setzt außerdem voraus, dass die Betroffenen, d. h. die Unterzeichner der Liste, kein schutzwürdiges Interesse am Ausschluss der Datenübermittlung an die Firma hatten. Das Schreiben mit der Unterschriftenliste war an die Gemeinde gerichtet. Ziel des Schreibens war, auf die Entscheidungsfindung der Gemeinde, respektive des Gemeinderats, dergestalt Einfluss zu nehmen, dass die Gemeinde im Bauleitplanverfahren kein Industriegebiet ausweist. Die Unterzeichner der Liste durften darauf vertrauen, dass ihre an die Gemeinde gerichteten persönlichen Daten von dieser nur zu dem übermittelten Zweck verwendet werden und nicht an das interessierte Unternehmen oder sonstige Dritte weitergegeben werden. Es konnte auch nicht ausgeschlossen werden, dass Mitarbeiter der Firma, die in der Gemeinde wohnen, und Personen, die beabsichtigen, sich bei der Firma zu bewerben, an der Unterschriftenaktion teilgenommen haben. Diese hatten ein schutzwürdiges Interesse daran, dass ihnen durch ihre Unterschriftsleistung keine Nachteile entstehen.

Die Schutzbedürftigkeit entfiel im Übrigen auch nicht etwa dadurch, dass Einwendungen, die im Bauleitplanverfahren im Rahmen der Beteiligung der Bürger vorgetragen werden, der Sache nach im Gemeinderat grundsätzlich öffentlich erörtert werden. Auch bei der Behandlung einer Angelegenheit nach Art. 52 Abs. 2 GO in öffentlicher Sitzung ist eine Bekanntgabe personenbezogener Daten nur in dem **erforderlichen Umfang** zulässig. Das bedeutete, dass zwar bei einer Behandlung des Schreibens im Gemeinderat die Unterschriftenliste den Gemeinderatsmitgliedern, die zur Verschwiegenheit verpflichtet waren, zur Kenntnis gegeben werden durfte. Unzu-

lässig wäre aber ein Verlesen der Unterschriftenliste in öffentlicher Gemeinderatssitzung gewesen. Wie bereits ausgeführt, muss der Bürger darauf vertrauen können, dass mit seinem Anliegen nur die zuständigen Stellen befasst werden und die Unterschriftenliste innerhalb der Gemeindeverwaltung und der zuständigen Entscheidungsgremien verbleibt. Es konnte also keine Rede davon sein, dass durch die Behandlung der Angelegenheit grundsätzlich in öffentlicher Sitzung die Namen und Anschriften der Unterzeichner der Unterschriftenliste nicht mehr schutzwürdig waren.

Zu dem Vortrag der Gemeinde, sie habe die Unterlagen an die „Vorhabensträgerin dieses Bauleitplanverfahrens“, die Firma XY, weitergegeben, habe ich darauf hingewiesen, dass Bauleitpläne **von der Gemeinde in eigener Verantwortung aufzustellen sind, sobald und soweit es für die städtebauliche Entwicklung und Ordnung** (der Gemeinde) **erforderlich ist** (§§ 1 Abs. 3 und 2 Abs. 1 BauGB). Im Verfahren ist es **alleinige Aufgabe der Gemeinde**, bei der Beteiligung der Bürger vorgebrachte Anregungen zu prüfen (§ 3 Abs. 2 Satz 4 BauGB). Das gilt auch im Verfahren für einen vorhabenbezogenen Bebauungsplan (§ 12 BauGB), das die Gemeinde auf Antrag eines Vorhabenträgers und auf der Grundlage eines von ihm vorgelegten Vorhaben- und Erschließungsplans durchführt.

Die Weitergabe des genannten Schreibens und der Unterschriftenliste sowie sonstiger im Rahmen der Bürgerbeteiligung an die Gemeinde gerichtete Schreiben mit personenbezogenen Daten an das Privatunternehmen habe ich nach Art. 31 Abs. 1 BayDSG beanstandet. Ein Absehen von der Beanstandung nach Art. 31 Abs. 3 BayDSG war mir nicht möglich, weil der Datenschutzverstoß nicht geringfügig war und durch die bereits erfolgte Bekanntgabe der Daten an die Firma auch nicht mehr rückgängig gemacht werden konnte.

8.11 Behandlung der Bewerberliste für Schöffen im Gemeinderat

Eine Gemeinde hat mich gefragt, ob die Auswahl der dem Amtsgericht vorzuschlagenden Personen für das Schöffenamt in öffentlicher oder nichtöffentlicher Gemeinderatssitzung zu erfolgen hat. Ich vertrete dazu folgende Auffassung:

Nach § 7 Abs. 3 der Gemeinsamen Bekanntmachung der Bayerischen Staatsministerien der Justiz und des Innern vom 06.12.1991 (AllMBl Nr. 1/1992) in der Fassung vom 15.09.1999 (AllMBl Nr. 21/1999) sind die für ein Schöffenamt eingehenden Bewerbungen dem Gemeinderat vorzulegen. Für die Aufnahme von Personen in die Vorschlagsliste für Schöffen ist die Zustimmung von zwei Dritteln der gesetzlichen Zahl der Mitglieder des Gemeinderats erforderlich (§ 7 Abs. 2 der Bekanntmachung).

Bei der Behandlung der Angelegenheit im Gemeinderat kommen zwangsläufig Angaben zur Person der Bewerber und zu ihren persönlichen und sachlichen Verhältnissen zur Sprache, soweit diese für die Berufung zum Schöffen und zur Auswahl aus Bewerbungen von Bedeutung sind. Zudem muss für die Auswahl der vorzuschlagenden Personen eine Bewertung der Bewerbungen im Verhältnis zueinander vorgenommen werden. Die Betroffenen haben daher ein erhebliches berechtigtes Interesse daran, dass die Angelegenheit in nichtöffentlicher Sitzung behandelt wird (Art. 52 Abs. 2 GO). Eine Behandlung in nichtöffentlicher Sitzung ist in einem solchen Fall auch erforderlich, um eine objektive und unbeeinflusste Amtsausübung der Gemeinderatsmitglieder bei einer derartigen Gelegenheit zu ermöglichen.

An dieser Bewertung ändert auch die Tatsache nichts, dass die dann beschlossene Vorschlagsliste gem. § 36 Abs. 3 GVG öffentlich aufzulegen ist, da diese Vorschlagsliste zum einen nur die angenommenen Bewerber, zum anderen aber auch von diesen nur die in § 36 Abs. 2 Satz 2 GVG bestimmten Daten aufführt.

8.12 Weitergabe eines Auszugs aus dem Heiratseintrag an einen ausländischen Staat

Ein Ehepaar hat mich gebeten, die Weitergabe eines Auszugs aus dem Heiratseintrag durch das Standesamt an ein ausländisches Konsulat datenschutzrechtlich zu überprüfen. Die betroffene Gemeinde nahm dazu wie folgt Stellung:

Anlässlich der Eheschließung der Petenten sei auch eine Mitteilung an das Geburtsstandesamt der Ehefrau im Ausland erfolgt. Der Standesbeamte habe nach der Beurkundung der Eheschließung Mitteilungen nach § 97 der Dienstanweisung an die davon betroffenen Standesämter zu machen. Diese Mitteilungen würden der vorgeschriebenen Fortschreibung der Personenstandsbücher dienen. Bei Beteiligung eines ausländischen Standesamts erfolge die Mitteilung über das zuständige Konsulat, hier in Form eines mehrsprachigen Auszugs aus dem Heiratseintrag. Dieser enthalte nur die notwendigen Angaben zur Fortführung (§ 97 Abs. 2 DA) und zwar Tag und Ort der Eheschließung, Namen, Vornamen, Tag und Ort der Geburt der Ehegatten, sowie Name nach der Eheschließung. Zwischen der Bundesrepublik Deutschland und dem ausländischen Staat seien im vorliegenden Fall für den Vollzug des Personenstandsgesetzes hauptsächlich folgende internationale Abkommen von Bedeutung: Das Europäische Beglaubigungsübereinkommen und das Wiener Konsularübereinkommen. Die Gemeinde wies außerdem darauf hin, dass die Petenten der Veröffentlichung ihrer Daten anlässlich ihrer Eheschließung im Gemeindeblatt zugestimmt hatten.

Diesen Sachverhalt habe ich datenschutzrechtlich wie folgt bewertet:

Die Weitergabe der personenbezogenen Daten der Petenten war zulässig, wenn sie im Vollzug einer Rechtsvorschrift erfolgt ist oder die Betroffenen in die Datenweitergabe eingewilligt hatten (Art. 15 Abs. 1 BayDSG).

Die Zustimmung zur Veröffentlichung von Daten anlässlich der Eheschließung im Gemeindeblatt der Gemeinde bezog sich auf einen anderen Sachverhalt und rechtfertigte deshalb nicht die Datenübermittlung an das ausländische Konsulat. Die Datenübermittlung erfolgte auch ohne Rechtsgrundlage.

Die in den personenstandsrechtlichen Vorschriften geregelten Mitteilungen zwischen den Standesbeamten betreffen grundsätzlich nur Mitteilungen an deutsche Standesbeamte. Die Mitteilung über Personenstandsfälle an ausländische Konsulate oder ausländische Standesämter setzt eine besondere Ermächtigung in Form eines von der Bundesrepublik Deutschland und dem jeweiligen ausländischen Staat ratifizierten bilateralen oder multilateralen Abkommens voraus. Dabei sind die Voraussetzungen und der Umfang der vereinbarten Übermittlung nach Maßgabe des jeweiligen Abkommens zu beachten. Daten, die über die Vereinbarung hinausgehen, dürfen nicht übermittelt werden.

Zwischen der Bundesrepublik Deutschland und dem im vorliegenden Fall betroffenen ausländischen Staat ist für standesamtliche Mitteilungen nur das Wiener Abkommen über konsularische Beziehungen vom 24.04.1963 (BGBl 1969 II S. 1585) zu beachten (siehe auch § 117 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden). Danach ist bei dem Tod eines Angehörigen eines Vertragsstaates dem Konsulat dieses Staates eine Sterbeurkunde zu übersenden. Das Abkommen sieht keine Mitteilung nach einer Eheschließung vor.

Die beiden anderen zwischen Deutschland und dem betroffenen ausländischen Staat für den standesamtlichen Bereich wirksamen Abkommen (das Europäische Beglaubigungsübereinkommen und das HAAGER Übereinkommen über den Zivilprozess) enthalten keine Mitteilungspflichten für die deutschen Standesbeamten.

Die Übersendung eines Auszugs aus dem Heiratseintrag an das ausländische Konsulat war demnach unzulässig und wurde von mir beanstandet.

8.13 Einsicht in staatsanwaltschaftliche Ermittlungsakten durch die Mitglieder eines kommunalen Gremiums

Ein Landkreis hat sich mit folgendem Sachverhalt an mich gewandt:

Ein Unternehmer, gegen den wegen unberechtigter Verrechnung von Leistungen gegenüber dem Landkreis ein Strafbefehl erlassen wurde, hat zur Wiedergutmachung des angerichteten Schadens einen Geldbetrag an den Landkreis überwiesen. Der zuständige Ausschuss des Landkreises hat daraufhin den Beschluss gefasst, dass „der Landkreis die Staatsanwaltschaft ersucht, die Ermittlungsakten und den ergangenen Strafbefehl zur Einsicht und zur Auswertung zur Verfügung zu stellen“. Die Staatsanwaltschaft hat auf das Ersuchen des Landkreises hin dem Landrat in dessen Funktion als Vertreter der Körperschaft des öffentlichen Rechts „Landkreis“ Ermittlungsakten sowie Beweismittelakten zur Einsicht zur Verfügung gestellt. In diese Akten wollte der zuständige Ausschuss des Landkreises Einsicht nehmen.

Aus den übermittelten Unterlagen der Staatsanwaltschaft ergaben sich nach den Feststellungen des Landrats eine Vielzahl sensibler personenbezogener Daten. So war z. B. aus den Ermittlungsdaten ersichtlich, inwieweit Personen bei der Anzeigeerstattung und Weiterleitung von Unterlagen an Polizei und Justiz mitgewirkt haben. Aus den Protokollen zahlreicher Zeugenvernehmungen ergaben sich geschützte personenbezogene Daten sowie Detailumstände von Vernehmungen. Den Unterlagen konnten ferner in großem Umfang Geschäftsgeheimnisse (z. B. Kalkulationsgrundlagen, Gesellschaftsanteilübertragungen, Mitarbeiterverdienste, Umsatzzahlen, Firmenausscheidungsgründe und damit verbundene Abfindungen) entnommen werden.

Ich habe den Vorgang datenschutzrechtlich wie folgt bewertet:

8.13.1 Datenübermittlung durch die Staatsanwaltschaft an den Landkreis

Auf das Ersuchen des Landkreises hin hat die Staatsanwaltschaft Ermittlungsakten und Beweismittelakten aus dem Strafverfahren gegen den Unternehmer dem Landrat zur Akteneinsicht überlassen. Rechtsgrundlage für die Datenübermittlung war § 406 e StPO. Diese Vorschrift ermöglicht die Akteneinsicht durch den Verletzten eines Strafverfahrens, soweit er hierfür ein berechtigtes Interesse darlegt.

Im vorliegenden Fall war der Landkreis Geschädigter eines Betrugsverfahrens durch falsche Abrechnungen eines Unternehmers. Die Akteneinsicht erschien erforderlich, um es dem Landkreis als Geschädigtem zu ermöglichen, den Schadensumfang aufgrund der durchgeführten Ermittlungen nachzuvollziehen und ggf. entsprechende Nachforderungen an den Schädiger stellen zu können sowie um sich über die Frage weiterer Geschäftsbeziehungen mit dem genannten Unternehmer schlüssig zu werden. Die von der Staatsanwaltschaft übermittelten Unterlagen durften vom Landkreis **zu diesem Zweck** genutzt werden. Als Datenempfänger war der Landkreis zur Beachtung der Zweckbindung der übermittelten Daten verpflichtet (Art. 18 Abs. 3, 17 Abs. 1 Nr. 2 BayDSG).

8.13.2 Einsichtnahme durch einen Ausschuss des Kreistages in Ermittlungsakten

Nach Art. 22 der Landkreisordnung wird der Landkreis durch den Kreistag verwaltet, soweit nicht vom Kreistag bestellte Ausschüsse über Kreisangelegenheiten beschließen oder der Landrat selbstständig entscheidet. Soweit danach dem Kreistag bzw. dem zuständigen Ausschuss die Entscheidung über eine evtl. Nachforderung sowie der Fortsetzung der Geschäftsbeziehung mit dem Schädiger obliegt, hat das zuständige Kreisorgan einen Anspruch auf die zur Beratung und Entscheidung **erforderlichen** Informationen, wozu auch die Einsichtnahme in Akten oder Aktenbestandteile gehören kann. **Insoweit** wäre dann auch die Weitergabe personenbezogener Daten zulässig (vgl. Masson/Samper Anm. 8 zu Art. 30 GO). Für die Weitergabe personenbezogener Daten ergibt sich dabei die Verpflichtung zur Beachtung des Grundsatzes der Erforderlichkeit aus Art. 17 Abs. 1 Nr. 1 BayDSG. Die Weitergabe personenbezogener Daten von der Kreisverwaltung an den Kreistag bzw. einen Ausschuss stellt eine Datennutzung im Sinne dieser Bestimmung dar. Wenn nach diesen Grundsätzen eine Akteneinsicht durch das Beschlussorgan in Frage kommt, hat deshalb vorher die Verwaltung durch entsprechende Maßnahmen zu gewährleisten, dass für die Entscheidung nicht erforderliche personenbezogene Daten auch nicht zur Kenntnis genommen werden können (Herausnahme dieser Aktenbestandteile oder Vorlage von geschwärzten Kopien).

Als Vorsitzender des Kreistages bzw. des Ausschusses entscheidet zunächst der Landrat nach pflichtgemäßem Ermessen, auf welche Weise er die Kreisräte über die zu behandelnden Beratungsgegenstände informieren will. Die Unterrichtung der Mandatsträger kann durch die Versendung von Sitzungsunterlagen, mündlichen Vortrag in der Sitzung und die Verteilung von Tischvorlagen erfolgen. Unterlagen mit Angaben zu sensiblen, in nichtöffentlicher Sitzung zu behandelnden Gegenständen, sollten nicht versandt, sondern ggf. nummeriert als Tischvorlage für die Dauer der Sitzung zur Verfügung gestellt und anschließend wieder eingesammelt werden. Soweit danach im vorliegenden Fall eine Einsichtnahme des zuständigen Kreisorgans in Unterlagen der Staatsanwaltschaft in Betracht kam, sollte diese während eines festgelegten Zeitraums vor der Sitzung in den Amtsräumen oder in der nichtöffentlichen Sitzung des Organs erfolgen. Dabei waren Vorkehrungen zu treffen, dass keine Kopien angefertigt und aus dem Amtsraum bzw. dem Sitzungssaal entfernt werden konnten. Vor einer Akteneinsicht waren die Unterlagen

der Staatsanwaltschaft unter dem Gesichtspunkt der Erforderlichkeit, wie oben ausgeführt, durchzusehen und bei der Vorlage entsprechend zu beschränken.

Eine Bitte im Ersuchen des Landkreises um Auskunft an die Staatsanwaltschaft, ob es als zulässig erachtet wird, den Ausschussmitgliedern bzw. den im Kreistag vertretenen politischen Gruppierungen Einblick in die Unterlagen zum Gebrauch gegenüber der Öffentlichkeit zu geben, habe ich zum Anlass genommen, gegenüber dem Landkreis darauf hinzuweisen, dass eine Übermittlung personenbezogener Daten aus den Unterlagen der Staatsanwaltschaft an die Öffentlichkeit unzulässig wäre und von mir beanstandet werden müsste. Ich habe in diesem Zusammenhang angeregt, die Mitglieder des zuständigen Kreisorgans ausdrücklich auf ihre Verschwiegenheitspflicht hinzuweisen.

8.13.3 Information der Öffentlichkeit

Zur Frage einer Information der Öffentlichkeit habe ich es im Hinblick auf die Bedeutung der Angelegenheit und die bereits in der Presse erfolgte Berichterstattung für zulässig erachtet, dass der Landkreis durch den Landrat oder den vom ihm Beauftragten die Öffentlichkeit über die **Höhe** einer evtl. Nachforderung bzw. die Feststellung, dass die Nachprüfung keinen weiteren Anspruch gegen den Schädiger ergeben hat, sowie über eine Entscheidung, ob die Geschäftsbeziehung mit dem Schädiger auch weiter aufrechterhalten wird, informiert (Art. 19 Abs. 1 Nr. 2 BayDSG).

8.14 Die neugierige Sekretärin

Wie schnell schutzwürdige personenbezogene Daten bei einem sorglosen Umgang innerhalb einer Kommune an Unbefugte und darüber hinaus sogar an die Öffentlichkeit gelangen können, zeigt der folgende Fall:

Ein homosexuelles Paar hatte beim Standesamt einer Stadt ein Aufgebot bestellt. Gegen die Ablehnung des Aufgebots hatte das Paar geklagt. Der zuständige Richter schilderte diesen Fall in anonymisierter Form, aber unter Nennung des Namens der Stadt, bei einem Lehrgang. An diesem Lehrgang hat auch eine Bedienstete der Stadt teilgenommen, die sich daraufhin beim Standesbeamten nach dem Fall erkundigt hat. Aus den Angaben, die der Standesbeamte ihr gegenüber gemacht hat, war es der Bediensteten möglich, die Betroffenen zu identifizieren. Auf einer privaten Feier hat sie einer dritten Person, bei der es sich zufällig um einen Bekannten des heiratswilligen Paares gehandelt hat, von dem Heiratsantrag erzählt. Die beiden Betroffenen haben sich, nachdem sie durch den gemeinsamen Bekannten von dem Vorgang Kenntnis erlangt hatten, an mich gewandt.

Die von mir dazu befragte Stadt bestätigte den Vorgang und teilte außerdem mit, die Bedienstete, die als Sekretärin in einem anderen Vorzimmer beschäftigt sei, habe sich in einem Ausbildungs- und Weiterbildungsverhältnis befunden. Im Rahmen der praktischen Ausbildung habe sie Zugang zu entsprechenden Daten gehabt.

Ich habe diesen Sachverhalt datenschutzrechtlich wie folgt bewertet:

- **Datenweitergabe innerhalb der Stadt**

Die Weitergabe von Informationen bezüglich des Antrags der Petenten auf Eheschließung durch den Standesbeamten an die Mitarbeiterin eines anderen Amtes der Stadt stellte datenschutzrechtlich eine Nutzung personenbezogener Daten dar (Art. 4 Abs. 7 BayDSG), die gem. Art. 15 Abs. 1 BayDSG einer gesetzlichen Grundlage bedurfte, da die Betroffenen darin nicht eingewilligt hatten.

Mangels spezialgesetzlicher Vorschriften richtete sich die Datennutzung nach Art. 17 BayDSG. Danach setzte die Weitergabe der Daten unter anderem voraus, dass sie zur Aufgabenerfüllung der Empfängerin bzw. des Standesamts erforderlich war (Art. 17 Abs. 1 BayDSG).

Die Bedienstete war als Sekretärin mit Vorzimmertätigkeiten betraut. Anhaltspunkte, dass sie die Daten hierfür benötigte, bestanden nicht. Auch soweit die Weitergabe der Daten zu Ausbildungszwecken der Bediensteten erfolgte, war es nicht erforderlich, dieser personenbezogene Daten der Petenten mitzuteilen. Es hätte vielmehr genügt, wenn die Bedienstete in anonymisierter Form unterrichtet worden wäre. Die Weitergabe der Daten vom Standesbeamten an die Sekretärin war daher rechtswidrig.

- **Datenübermittlung an einen privaten Dritten**

Die Bekanntgabe des Heiratsantrags der Petenten durch die Sekretärin auf einer privaten Feier gegenüber einer dritten Person war eindeutig rechtswidrig. Es fehlte erkennbar schon an einem berechtigten Interesse des Dritten an den übermittelten Daten (Art. 19 Abs. 1 Nr. 2 BayDSG). Darüber hinaus hatten die Betroffenen ein erhebliches Interesse daran, dass zum einen niemand gegen ihren Willen von ihren Heiratsplänen Kenntnis erlangte und, dass zum anderen ihre Homosexualität, die sich aus der Bekanntgabe ihrer Heiratsabsichten zwangsläufig ergab, nicht offengelegt wurde. Es war insbesondere nicht auszuschließen, dass den Betroffenen dadurch persönliche bzw. ggf. auch berufliche Nachteile entstehen konnten. Allgemein ist darauf hinzuweisen, dass ein Bürger, der sich mit einem Anliegen an die Verwaltung wendet, darauf vertrauen können muss, dass sein Anliegen entsprechend der einschlägigen gesetzlichen Bestimmungen behandelt wird und im Bereich der zuständigen Stelle(n) der Verwaltung verbleibt.

Die rechtswidrige Weitergabe der Daten über den Eheschließungsantrag durch den Standesbeamten an die Sekretärin sowie deren Bekanntgabe an einen Dritten habe ich gem. Art. 31 Abs. 1 BayDSG beanstandet. Von der Beanstandung konnte nicht abgesehen werden, da beide Vorgänge einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellten.

9 Einwohnermeldewesen

9.1 Weitergabe von Melderegisterdaten an Adressbuchverlage

Ich erhalte immer wieder Beschwerden von Bürgern, die mit der Veröffentlichung ihrer Daten in Adressbüchern nicht einverstanden sind. Ich weise deshalb nochmals auf Folgendes hin:

Nach Art. 35 Abs. 3 des Meldegesetzes (MeldeG) darf die Meldebehörde Adressbuchverlagen Auskunft über Vor- und Familiennamen, den Doktorgrad und die Anschriften sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, erteilen, es sei denn, der Betroffene hat dieser Weitergabe seiner Daten widersprochen. Die Bürger müssen bei der Anmeldung von der Meldebehörde auf ihr Widerspruchsrecht hingewiesen werden. Nach meinen Erfahrungen ist dieser Hinweis, der häufig auch schon Jahre zurückliegt, aber nicht ausreichend. Vielen Bürgern ist ihr Widerspruchsrecht nicht bekannt. Ich empfehle deshalb den Gemeinden, über die Hinweispflicht des Art. 35 Abs. 3 Satz 3 MeldeG hinaus die Bürger rechtzeitig vor einer beabsichtigten Weitergabe ihrer Meldedaten an Adressbuchverlage in geeigneter Weise, z. B. durch eine amtliche Bekanntmachung in der Presse, auf ihr Widerspruchsrecht hinzuweisen (vgl. auch Nr. 35.4 der Vollzugsbekanntmachung zum Meldegesetz). Zusätzlich zu den regelmäßigen Hinweisen auf das Widerspruchsrecht der Bürger in meinen Tätigkeitsberichten habe ich im Berichtszeitraum dazu auch eine Pressemitteilung veröffentlicht.
In diesem Zusammenhang möchte ich auch darauf hinweisen, dass die Kommunen zur Herausgabe von Meldedaten an Adressbuchverlage nicht verpflichtet sind. Art. 35 Abs. 3 Satz 1 MeldeG enthält eine Übermittlungs**befugnis** („darf“). Die Erteilung von Auskünften steht daher im Ermessen der Kommunen.

9.2 Vermeidung von Fehlern bei einem Wechsel des EDV-Programms zur Verwaltung der Einwohnermeldedaten

Im Berichtszeitraum haben sich Bürger beschwert, deren Daten in Adressbüchern veröffentlicht wurden, obwohl sie der Weitergabe nach Art. 35 Abs. 3 MeldeG widersprochen hatten. Die Überprüfung der Vorwürfe hat ergeben, dass die betroffenen Gemeinden ihre in den Einwohnermeldeämtern eingesetzten EDV-Verfahren auf neue Verfahren umgestellt hatten. Bei der Übernahme der Datenbestände waren Sperrvermerke nicht beachtet worden. Trotz durchgeführter Stichproben waren die Fehler bei der Weiterleitung der Daten an die Adressbuchverlage nicht bemerkt worden. Die Veröffentlichung ihrer Daten in den Adressbüchern und der Verstoß gegen die Sperrvermerke hat bei den betroffenen Bürgern zu einer erheblichen Verärgerung und zu den Beschwerden geführt. Ich empfehle den Gemeinden, bei Programmänderungen bzw. Neuprogrammierungen durch technisch-organisatorische Maßnahmen (umfassende Teststrategien und Qualitätssicherungsmaßnahmen) sicherzustellen, dass die Voraussetzungen für Auskunftserteilungen im Rahmen des Art. 35 MeldeG eingehalten und sowohl Widersprüche nach Art. 35 MeldeG als auch Auskunftssperren nach Art. 34 MeldeG weiterhin beachtet werden.

9.3 Unzulässige Speicherung des früheren Namens von minderjährigen adoptierten Kindern im Melderegister

Im Berichtszeitraum wurden mir innerhalb kurzer Zeit zwei schwerwiegende Verstöße gegen das Adoptionsgeheimnis bekannt. Die Überprüfungen haben ergeben, dass bei Minderjährigenadoptionen in den Melderegistern der beiden betroffenen Gemeinden unter der Rubrik „Früherer Name“ der Geburtsname der adoptierten Kinder gespeichert war. Als Folge der nicht durchgeführten Löschungen wurde der Geburtsname im Online-Verfahren an die Polizei übermittelt, anschließend wurden die Betroffenen im Rahmen der Abklärung ihrer Personalien in einem Verfahren von der Polizei auch zu ihrem früheren Namen befragt.

Ich habe diese Vorgänge datenschutzrechtlich wie folgt bewertet:

Nach Art. 11 Abs. 1 Satz 1 MeldeG hat die Meldebehörde gespeicherte Daten zu löschen, wenn sie zur Erfüllung der der Meldebehörde obliegenden Aufgaben nicht mehr erforderlich sind. Die Speicherung des früheren Namens eines minderjährigen adoptierten Kindes ist weder zum Nachweis seiner Identität noch für andere Aufgaben der Meldebehörde notwendig. Dies ergibt sich daraus, dass ein minderjähriges Kind regelmäßig noch nicht am Rechtsverkehr teilgenommen hat. Es gibt auch keine zwingende Notwendigkeit zur Offenbarung des früheren Namens gegenüber anderen Behörden, da sich diese erforderlichenfalls an das zuständige Standesamt wenden können (vgl. Medert/Süßmuth/Dette-Koch, Melderecht des Bundes und der Länder, § 21 MRRG Rdnr. 79). Das Bayerische Staatsministerium des Innern hat deshalb in Ziff. 3.1.5 der Vollzugsbekanntmachung zum Bayerischen Meldegesetz bestimmt, dass bei der Annahme als Kind (Adoption) im Zusammenhang mit dem neuen Namen weder der vor der Adoption geführte Name noch ein sonstiger Hinweis auf die Adoption im Melderegister gespeichert werden darf. Wenn der Adoptierte zum Zeitpunkt der Adoption bereits volljährig war, ist der frühere Name im Nebenregister zu speichern.

Die Bekanntgabe eines Adoptionsverhältnisses kann sowohl für den minderjährigen Adoptierten wie auch für dessen Adoptiveltern ganz erhebliche nachteilige Folgen haben, insbesondere wenn der Adoptierte erstmals durch eine polizeiliche Befragung von seiner Adoption erfährt. Die Da-

tenschutzverstöße habe ich beanstandet. Da es sich hier möglicherweise nicht nur um zwei Einzelfälle gehandelt hat, empfehle ich den Gemeinden, ihre Melderegister auf unzulässige Speicherungen von Minderjährigenadoptionen hin zu überprüfen.

9.4 Weitergabe von Melderegisterdaten innerhalb der Gemeindeverwaltung im Wege des Online-Zugriffs

Mehrere Gemeinden haben mich um Auskunft gebeten, ob Gemeindebediensteten, die nicht im Meldeamt beschäftigt sind, ein Lesezugriff auf die Meldedaten eingeräumt werden darf. Ich habe den Gemeinden Folgendes mitgeteilt:

Nach Art. 31 Abs. 7 i.V.m. Abs. 1 MeldeG dürfen die in Art. 3 Abs. 1 MeldeG genannten Daten und Hinweise innerhalb der Gemeinde weitergegeben werden, wenn dies zur Aufgabenerfüllung der Meldebehörde bzw. des Bediensteten, der die Daten erhält, erforderlich ist. Für die Weitergabe und Einsichtnahme von Daten und Hinweisen nach Art. 3 Abs. 2 MeldeG ist Art. 31 Abs. 2 und 6 MeldeG zu beachten (Art. 31 Abs. 7 Satz 3 MeldeG).

Da es sich bei der Weitergabe von Meldedaten innerhalb der Gemeinde um eine Datennutzung und nicht um eine Datenübermittlung handelt, dürfen die Daten abweichend von Art. 31 Abs. 4 MeldeG auch regelmäßig weitergegeben werden. Dies gilt auch für automatisierte Abrufverfahren, die als regelmäßige Datenweitergabe anzusehen sind (vgl. Nr. 31.9 der Vollzugsbekanntmachung zum Meldegesetz).

Die Einrichtung eines automatisierten Abrufverfahrens ist allerdings nur dann zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist. Das ist der Fall, wenn der betreffende Mitarbeiter zur Erfüllung seiner dienstlichen Aufgaben ständig einen Zugriff auf das Melderegister benötigt. Soweit danach die Einrichtung eines automatisierten Abrufverfahrens zulässig ist, ist darauf zu achten, dass der Zugriff auf die zur Aufgabenerfüllung erforderlichen Daten beschränkt wird.

10 Ausländerwesen

10.1 Ausschreibungen nach Art. 96 des Schengener Durchführungsübereinkommens (SDÜ)

Als eine Ausgleichsmaßnahme für den Wegfall der Binnengrenzkontrollen in Europa wurde auf der Grundlage der Art. 92 ff. des Schengener Durchführungsübereinkommens ein gemeinsames Informations- und Fahndungssystem (SIS) eingerichtet. Es handelt es sich hier um eine gemeinsam betriebene automatisierte Fahndungsdatei, mittels derer in allen Schengen-Staaten gleichzeitig nach bestimmten Personen oder Gegenständen gesucht werden kann.

Jeder Bürger kann in jedem der Schengen-Staaten über die zu seiner Person im SIS gespeicherten Daten Auskunft verlangen (Art. 109 SDÜ). Die angesprochene Kontrollinstanz muss sich dann mit der Kontrollinstanz desjenigen Staates in Verbindung setzen, der eine Ausschreibung vorgenommen hat. Bei Ausschreibungen im SIS, die durch Ausländerbehörden der Bundesrepublik Deutschland vorgenommen wurden, leitet der Bundesbeauftragte für den Datenschutz die Anfrage an den zuständigen Landesbeauftragten für den Datenschutz weiter. Nach Eingang der Stellungnahme des beteiligten Landesbeauftragten für den Datenschutz unterrichtet der Bundesbeauftragte für den Datenschutz die ausländische Kontrollinstanz über das Ergebnis der datenschutzrechtlichen Kontrolle.

In mehreren Fällen, die mir der Bundesbeauftragte für den Datenschutz in diesem Verfahren zugeleitet hat, musste ich feststellen, dass abgelehnte Asylbewerber, die ihrer Ausreisepflicht nicht nachgekommen sind, zur Festnahme im SIS ausgeschrieben worden sind.

Art. 96 SDÜ lässt für die Ausländerbehörden eine Ausschreibung in diesem Informationssystem unter bestimmten Voraussetzungen zum Zwecke der Einreiseverweigerung, nicht aber auch zur Festnahme zu. Nach Art. 96 Abs. 3 SDÜ kommt die Ausschreibung zur Einreiseverweigerung dann in Frage, wenn ein Einreiseverbot in Folge einer Ausweisung oder Abschiebung besteht. Darüber hinaus kann die Ausländerbehörde im Einzelfall eine Ausschreibung nach Art. 96 Abs. 2 SDÜ dann veranlassen, wenn eine Ausweisung beabsichtigt gewesen, aber mangels Bekanntgabe unterblieben ist, weil der Ausländer ausgereist oder untergetaucht ist. Diese Voraussetzungen sind bei Ausländern, die lediglich ihrer Ausreiseverpflichtung nicht oder nicht in kontrol-

lierter Weise nachkommen, nicht gegeben. Die mit der Ausschreibung zur Festnahme verbundene Datenspeicherung war somit unzulässig.

Auf meine Anregung hin hat das Bayerische Staatsministerium des Innern mit Rundschreiben vom 06.12.1999 die nachgeordneten Behörden auf die Rechtslage hingewiesen und gebeten, dafür Sorge zu tragen, dass Speicherungen im SIS nur unter den rechtlichen Voraussetzungen des Art. 96 SDÜ und unter Beachtung der Allgemeinen Anwendungshinweise zum Schengener Durchführungsübereinkommen (AAH-SDÜ) veranlasst und nicht zulässige Speicherungen gelöscht werden.

10.2 Überprüfung von Scheinehen

Im Berichtszeitraum hat sich die Presse mit der Frage an mich gewandt, was die Ausländerbehörden aus datenschutzrechtlicher Sicht bei der Überprüfung von Scheinehen beachten müssen.

Eine Scheinehe liegt auch vor, wenn mit der Ehe eines deutschen Staatsangehörigen mit einem Angehörigen eines Drittstaats allein der Zweck verfolgt wird, die Rechtsvorschriften über die Einreise und den Aufenthalt von Angehörigen dritter Staaten in die Bundesrepublik Deutschland zu umgehen und dem Drittstaatsangehörigen eine Aufenthaltsgenehmigung oder -erlaubnis in der Bundesrepublik Deutschland zu verschaffen.

Nach der Entschließung des Rats der Europäischen Union vom 04.12.1997 sind die Mitgliedstaaten der EU verpflichtet, Maßnahmen zur Bekämpfung von Scheinehen zu ergreifen. Nr. 3 der Entschließung lautet wie folgt: „Begründen bestimmte Faktoren den Verdacht, dass es sich um eine Scheinehe handelt, so stellen die Mitgliedstaaten einem Angehörigen eines Drittstaats eine Aufenthaltsgenehmigung oder -erlaubnis aufgrund einer Eheschließung erst dann aus, wenn die nach dem innerstaatlichen Recht zuständigen Behörden überprüft haben, dass es sich bei der Ehe nicht um eine Scheinehe handelt und die übrigen Voraussetzungen im Zusammenhang mit der Einreise und dem Aufenthalt erfüllt sind. Diese Überprüfung kann ein getrenntes Gespräch mit jedem der beiden Ehegatten umfassen."

In der Bundesrepublik Deutschland wurde in § 1310 Abs. 1 Satz 2 BGB für die Standesbeamten eine Mitwirkungsverbot bei Scheinehen normiert. Zum Vollzug dieser Bestimmung hat das Bayerische Staatsministerium des Innern mit Rundschreiben vom 19.10.1998, Az.: IA3-2005.2-23, an dessen Erstellung ich beteiligt worden bin, den nachgeordneten Behörden Hinweise gegeben.

Des Weiteren haben die Ausländerbehörden im Verfahren der Erteilung bzw. des Entzugs einer Aufenthaltserlaubnis nach § 17 Abs. 1 des Ausländergesetzes zu prüfen, ob eine Scheinehe vorliegt. Dabei haben die Ausländerbehörden u. a. Folgendes zu beachten:

- Eine Überprüfung ist nur zulässig, wenn der Ausländerbehörde konkrete Anhaltspunkte für eine Scheinehe vorliegen. Diese dürfen nicht das Ergebnis eigener Ermittlungen der Ausländerbehörde zu diesem Zweck sein, sondern müssen dieser auf andere Weise, z. B. aus dem Verhalten oder Erklärungen der Betroffenen oder aus Schriftstücken, die ihr vorgelegt werden, bekannt geworden sein. Eine systematische Überprüfung aller Anträge auf Erteilung einer Aufenthaltserlaubnis und Ermittlungen zur Verdachtsfindung sind also unzulässig. Die Entschließung des Rats der Europäischen Union vom 04.12.1997 und das Rundschreiben des Innenministeriums vom 19.10.1998 enthalten beispielhafte Aufzählungen, in welchen Fällen konkrete Anhaltspunkte für eine Scheinehe vorliegen.

- Eine Befragung der Betroffenen ist erst nach Vorliegen konkreter Anhaltspunkte zulässig (vgl. § 5 Abs. 4 des Personenstandsgesetzes für Befragungen durch den Standesbeamten).

- Die Betroffenen sind vor der Befragung darauf hinzuweisen, dass die Datenerhebung zur Prüfung erfolgt, ob eine Scheinehe vorliegt (Angabe des Erhebungszwecks). Außerdem sind sie auf die Freiwilligkeit ihrer Angaben und ihre Obliegenheiten nach § 70 des Ausländergesetzes hinzuweisen (Art. 16 Abs. 3 Sätze 1 und 2 BayDSG).

- Die Befragung darf nicht schematisch nach Katalog, sondern nur in dem erforderlichen Umfang erfolgen (vgl. § 5 Abs. 4 des Personenstandsgesetzes).

- Fragen, die in unzulässiger Weise in das allgemeine Persönlichkeitsrecht eingreifen würden, sind unzulässig. Das sind insbesondere Fragen, die den Intimbereich berühren.

- Die Standesbeamten können im Vollzug des Eheschließungsrechts zur Verhinderung von Scheinehen auch eine Stellungnahme der zuständigen Ausländerbehörde einholen, soweit das zu ihrer Aufgabenerfüllung erforderlich ist. Dabei ist zu beachten, dass die Anforderung und Übersendung der vollständigen Ausländerakten unzulässig ist, weil diese auch personenbezogene Daten enthalten, die die Standesbeamten zur Überprüfung, ob eine Scheinehe beabsichtigt ist, nicht benötigen.

11 Steuerverwaltung

11.1 Anwendbarkeit des Landesdatenschutzgesetzes im Besteuerungsverfahren

Bereits seit längerer Zeit ist zwischen dem Staatsministerium der Finanzen und mir die Anwendbarkeit des Landesdatenschutzgesetzes im Besteuerungsverfahren strittig. Das Staatsministerium vertritt die Auffassung, dass das Datenschutzrecht durch die Abgabenordnung abschließend geregelt sei. Es weist darauf hin, dass sich auch die AO-Referatsleiter des Bundes und der Länder mehrfach mit dieser Rechtsfrage befasst hätten. Sie seien dabei zu dem Ergebnis gekommen, dass für die Anwendung des Bundesdatenschutzgesetzes bzw. der Landesdatenschutzgesetze im Besteuerungsverfahren kein Raum bleibe.

Ich halte diese Rechtsauffassung für nicht zutreffend.
Das Bayerische Datenschutzgesetz tritt nach Art. 2 Abs. 7 nur dann zurück, „soweit besondere Rechtsvorschriften über den Datenschutz auf personenbezogene Daten anzuwenden sind“. Hierzu führt der Kommentar zum Bayer. Datenschutzgesetz Wilde/Ehmann/Niese/Knoblauch (Art. 2, Rn. 79) folgendes aus:

„Das BayDSG wird allerdings immer nur im Rahmen des tatsächlichen Umfangs der Spezialnormen verdrängt. Soweit die Spezialnormen keine Regelung treffen, gilt das BayDSG. Ist bereichsspezifisch also z.B. nur die Zulässigkeit von Datenübermittlungen geregelt, so werden zwar die Art. 18 bis 21 BayDSG verdrängt, im Übrigen bleibt das BayDSG jedoch anwendbar. Es ist also keinesfalls so, dass ein Spezialgesetz, das datenschutzrechtliche Vorschriften enthält, das BayDSG schon allein deshalb insgesamt verdrängt. Verdrängen können nur die datenschutzrechtlich relevanten spezialgesetzlichen Paragraphen oder Artikel (ggf. nur deren einzelne Absätze oder Sätze) die ihnen jeweils entsprechenden (d.h. die gleiche konkrete Regelungsmaterie betreffenden) Bestimmungen des BayDSG.“

Beispielhaft kann die Anwendbarkeit des Bayer. Datenschutzgesetzes im Besteuerungsverfahren anhand der mir gem. Art. 30 BayDSG – insbesondere Art. 30 Abs. 2 Satz 1 BayDSG – zustehenden und von mir auch in Anspruch genommenen Kontrollkompetenz bei Landesfinanzbehörden dargelegt werden.

Würde die vom Staatsministerium geäußerte Rechtsauffassung zutreffen, wäre diese Kontrollkompetenz nicht gegeben, da in der Abgabenordnung entsprechende Regelungen fehlen. Ich gehe aber davon aus, dass das Staatsministerium meine Kontrollrechte im Besteuerungsverfahren nicht ernstlich in Zweifel ziehen möchte. Derartige Einwendungen wurden in der Vergangenheit im Vorfeld der zahlreichen rechtlichen und technisch-organisatorischen Prüfungen von im Geschäftsbereich dem Staatsministerium nachgeordneten Behörden auch nicht gemacht. Ich sehe meine Rechtsauffassung, im übrigen auch durch ein rechtskräftiges Urteil des **Finanzgerichts** Köln vom 18.12.11999, 2K 382/96, voll und ganz bestätigt. Das Finanzgericht führt im Hinblick auf ein Auskunftsverlangen gegenüber dem Bundesamt für Finanzen aus:

„Die Anwendbarkeit des BDSG ist ... nicht durch § 1 Abs. 4 BDSG ausgeschlossen. Danach ist das BDSG nicht anwendbar, soweit in anderen Gesetzen spezielle Regelungen enthalten sind. Diese Subsidiaritätsklausel greift nur bei Tatbestandskonkurrenz... Für einen Auskunftsanspruch gegen den Beklagten gibt es keine spezielle Regelung in anderen Gesetzen. Insbesondere § 30 AO enthält eine solche nicht ... .Über einen Anspruch des Steuerpflichtigen gegenüber einer Finanzbehörde auf Mitteilung der über ihn gespeicherten Daten sagt die Vorschrift überhaupt nichts aus. Es ist offensichtlich keine Frage des Steuergeheimnisses, wenn ein Steuerpflichtiger über seine Daten von einer Finanzbehörde Auskunft verlangt.“

Dazu kommt, dass die auch heute noch wesentliche Fassung der Abgabenordnung vom 16.03.1976 stammt und damit zeitlich vor dem Erlass des Bundesdatenschutzgesetzes, der Landesdatenschutzgesetze und dem Volkszählungsurteil des Bundesverfassungsgerichtes mit seinen klaren Aussagen zum informationellen Selbstbestimmungsrecht liegt. Zudem stellt das Datenschutzrecht in Bezug auf den Datenschutz jedenfalls in weiten Teilbereichen das speziellere Gesetz dar.

Ich muss mit aller Entschiedenheit einer Rechtsauffassung entgegentreten, die im Besteuerungsverfahren alle durch die Datenschutzgesetze geschaffenen Schutzrechte des Bürgers (Auskunftsanspruch, Berichtigungsanspruch, Löschungsanspruch, Anspruch auf Sperrung, Anspruch auf Schadensersatz) verneint, ohne gleichzeitig auf eine speziellere gesetzliche Regelung **zum gleichen Sachverhalt** verweisen zu können. Einer Unterstellung, dass dieser Verlust von Bürger-

rechten gewollt und vom Gesetzgeber beim Erlass der Abgabenordnung bedacht worden sei, ist schon im Hinblick auf den Zeitpunkt des Erlasses der Abgabenordnung unzutreffend.

Soweit die Finanzverwaltung eine Notwendigkeit für vom allgemeinen Datenschutzrecht abweichende Regelungen sieht, verweise ich auf die seit Jahren vergeblichen Aufforderungen der Datenschutzbeauftragten des Bundes und der Länder, eine Novelle der Abgabenordnung in die Wege zu leiten.

11.2 Elektronische Steuererklärung – ELSTER

Bereits in meinem 18. Tätigkeitsbericht habe ich aus technisch-organisatorischer Sicht zum Projekt ELSTER Stellung genommen (Nr. 19.3.12). Mit ELSTER verfolgt die Finanzverwaltung das Ziel, die elektronische Abgabe von Steuererklärungen zu ermöglichen. In diesem Zusammenhang stehen auch Überlegungen zur Schaffung einer elektronischen Lohnsteuerkarte, auf die ich in einem gesonderten Beitrag nachfolgend eingehe (Nr. 11.3).

Ich bin mir mit dem Bundesbeauftragten und den anderen Landesbeauftragten für den Datenschutz einig, dass gegen die Durchführung des Verfahrens ELSTER in seiner augenblicklichen Form keine grundsätzlichen Bedenken bestehen.

Die Abgabeordnung sieht in § 150 Abs. 6 AO auch die Möglichkeit vor, dass Steuererklärungen oder sonstige für das Besteuerungsverfahren erforderliche Daten ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermittelt werden können. Ein derartiges Verfahren ist aber an den Erlass einer entsprechenden Rechtsverordnung gebunden.
Die bisher aufgrund der Ermächtigung des § 150 Abs. 6 AO erlassenen Verordnungen sind in der augenblicklichen Fassung nicht auf die Abgabe von Steuererklärungen mittels des Verfahrens ELSTER anwendbar. Die 1999 im BStBl. I S. 1051 veröffentlichten „Grundsätze für die elektronische Übermittlung von Steuererklärungsdaten“ stellen lediglich Verwaltungsvorschriften dar und genügen damit nicht den Bestimmungen des § 150 Abs. 6 AO.

Verschiedene Steuergesetze sehen für eine rechtsverbindliche Abgabe einer Steuererklärung die eigenhändige Unterschrift vor. Für die Abgabe von Einkommensteuererklärungen bspw. besteht eine derartige Verpflichtung aufgrund § 25 Abs. 3 Satz 4 u. 5 EStG. Zwar ist im Rahmen des Signaturgesetzes (SigG) vom 22.07.1997 eine Möglichkeit geschaffen worden, die Unterschrift durch eine digitale Signatur zu ersetzen, eine entsprechende technische Infrastruktur zur Umsetzung fehlt aber zum gegenwärtigen Zeitpunkt.

Zu den elektronisch übermittelten Erklärungsdaten muss deshalb augenblicklich parallel eine komprimierte papierene Einkommensteuererklärung abgegeben werden. Nur diese ist für den Steuerpflichtigen rechtlich bindend.
Die Finanzverwaltung sieht aufgrund dieser Sachlage deshalb augenblicklich keine Notwendigkeit zum Erlass der erwähnten Verordnung. In § 150 Abs. 6 AO wird aber nicht nur die rechtsverbindliche elektronische Abgabe einer Steuererklärung an den Erlass einer entsprechenden Verordnung gebunden, sondern auch die ganz oder teilweise elektronische Übermittlung von sonstigen für das Besteuerungsverfahren erforderlichen Daten. Derartige Daten werden bei der Nutzung von ELSTER zweifelsfrei übermittelt, so dass der Erlass einer Rechtsverordnung zwingend notwendig ist.

Die Verordnung muss insbesondere Inhalt, Verarbeitung und Sicherung der zu übermittelnden Daten bestimmen. Darüber hinaus muss es dem Steuerpflichtigen überlassen bleiben, ob er seine Steuererklärung in der herkömmlichen Papierform oder elektronisch abgeben will.

Ich habe das Staatsministerium der Finanzen von meiner Rechtsauffassung in Kenntnis gesetzt und gebeten, sich für den alsbaldigen Erlass der angesprochenen Verordnung einzusetzen.

11.3 Elektronische Lohnsteuerkarte

In meinen Ausführungen zum Projekt ELSTER habe ich darauf hingewiesen, dass Ziel des Verfahrens u.a. ist, (Einkommen-)Steuererklärungen vollelektronisch bei der Finanzverwaltung einzureichen. Haupthinderungsgründe für derartige vollelektronische Steuererklärungen sind zum einen die in verschiedenen Steuergesetzen vorgeschriebene eigenhändige Unterschrift - die Nutzbarkeit von digitalen Signaturen ist noch nicht gegeben - zum anderen die vielfach den Steuererklärungen beizufügenden Belege und Bescheinigungen. Hier sind in erster Linie die für eine weit überwiegende Mehrzahl von Steuerpflichtigen relevanten Lohnsteuerkarten zu nennen.

Die Finanzverwaltung arbeitet deshalb mit Hochdruck an einem Verfahren für eine elektronische Lohnsteuerkarte. Nach Ansicht der Finanzverwaltung soll die elektronische Lohnsteuerkarte in einer ersten Phase nur ein Angebot an den Arbeitgeber darstellen. Zu einem späteren Zeitpunkt wird jedoch eine Verpflichtung zur elektronischen Übermittlung angestrebt.

Augenblicklich hat der Arbeitgeber aufgrund § 41 b Abs. 1 S. 4 EStG dem Arbeitnehmer die Lohnsteuerbescheinigung auszuhändigen, wenn das Dienstverhältnis vor Ablauf des Kalenderjahres beendet wird oder der Arbeitnehmer zur Einkommensteuer veranlagt wird. In den übrigen Fällen hat der Arbeitgeber die Lohnsteuerbescheinigung dem Betriebsstättenfinanzamt einzureichen.

Grundsätzlich sollte auch künftig an diesem Informationsfluss festgehalten werden. Soweit Steuerpflichtige künftig an einer vollelektronischen Abgabe ihrer Einkommensteuererklärung interessiert sind, sollten sie sich die Eintragungen in der Lohnsteuerbescheinigung von ihrem Arbeitgeber elektronisch zur Verfügung stellen lassen bzw., um etwaigen Bedenken der Finanzverwaltung zur nachträglichen Änderung der bescheinigten elektronischen Daten zu begegnen, in eine elektronische Übermittlung der Lohnsteuerbescheinigung an das für sie zuständige Finanzamt einwilligen.

Die Finanzverwaltung sieht zum jetzigen Verfahrensstand nur eine direkte Datenübermittlung vom Arbeitgeber an das für den Arbeitnehmer zuständige Finanzamt vor. Eine Wahlmöglichkeit für den Steuerpflichtigen soll nicht bestehen.

Mit der vorgesehenen direkten Übermittlung der Lohnsteuerdaten vom Arbeitgeber an die Finanzverwaltung ohne Einwirkungsmöglichkeit durch den Arbeitnehmer wird vom Grundsatz des Vorrangs der Datenerhebung beim Betroffenen (vgl. § 93 Abs. 1 Satz 2 AO) abgewichen. Dieser Eingriff in das informationelle Selbstbestimmungsrecht ist nur im überwiegenden **Allgemein**interesse und nur aufgrund eines normenklaren Gesetzes zulässig. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten (vgl. Urteil des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz, BVerfGE 65,1/44). Entsprechende Darlegungen der Finanzverwaltung zu den genannten Voraussetzungen fehlen. Nach den bisher vorgetragenen Argumenten ist das von der Finanzverwaltung dargelegte Konzept für eine elektronische Lohnsteuerkarte einseitig auf die eigenen Belange und jene der Arbeitgeber abgestellt.

Für Zwecke der Zuordnung der eingegangenen elektronischen Lohnsteuerdaten hat die Finanzverwaltung die Verwendung verschiedener Ordnungsbegriffe erwogen. So war daran gedacht, die Sozialversicherungsnummer für die Zuordnung zu verwenden. Ich war mir mit dem Bundesbeauftragten und den übrigen Landesbeauftragten für den Datenschutz einig, dass eine etwaige Änderung des § 18 f SGB IV als verfassungsrechtlich bedenklich anzusehen wäre. Die Erschließung der bei den Sozialversicherungsträgern und bei der Finanzverwaltung vorgehaltenen Datenbestände mittels eines einheitlichen Ordnungsmerkmales würde letztendlich der Einführung eines, aufgrund der bereits erwähnten Entscheidung des Bundesverfassungsgerichts nicht zulässigen, allgemeinen Personenkennzeichens sehr nahe kommen. Die Finanzverwaltung hat unter diesem Eindruck von der Verwendung der Sozialversicherungsnummer für ihre Zwecke Abstand genommen. Nach neueren Überlegungen ist nun an die Verwendung einer elektronisch vorgegebenen Taxpayer Identification Number (eTIN) gedacht. Dabei handelt es sich um eine personenbezogene lebenslange Nummer, die von einer Software unter zahlenmäßiger Verschlüsselung verschiedener Grundangaben (Name, Vorname, Geburtstag, Geburtsort) ermittelt wird.

Ich habe darauf hingewiesen, dass die Einführung und insbesondere die weitere Verwendung der sog. eTIN auf eine gesetzliche Grundlage, vergleichbar den zur Sozialversicherungsnummer erlassenen Bestimmungen in §§ 18 f, 18 g SGB IV, gestellt werden müsste.

Zu bedenken ist auch, dass die von mir eingangs erwähnte Einwilligungslösung auch die Angabe der jeweiligen persönlichen Steuernummer umfassen könnte, was die Schaffung eines neuen Ident-Merkmals unnötig machen würde.

Neben normenklaren Regelungen (Hinweis auf § 150 Abs. 6 AO und § 41 b Abs. 1 EStG) muss auch sichergestellt werden, dass Arbeitnehmern bei Einführung der elektronischen Lohnsteuerkarte die gesetzlich zu bescheinigenden Merkmale zusätzlich in Papierform zur Verfügung gestellt werden, um etwaige Fehlbescheinigungen des Arbeitgebers bzw. fehlerhafte Eingaben im Steuerbescheid erkennen zu können.

Für den Arbeitnehmer ist positiv zu werten, dass bei einem Arbeitsplatzwechsel eine Kenntnisnahme der bisher bescheinigten Lohnsteuerdaten durch den neuen Arbeitgeber derzeit nicht vorgesehen ist.

Ich habe gegenüber dem Staatsministerium der Finanzen deutlich gemacht, dass ich hinsichtlich weiterer Überlegungen zur Einführung einer elektronischen Lohnsteuerkarte einen kritischen Dialog für erforderlich halte.

11.4 Aufbewahrungs- und Speicherfristen in der Finanzverwaltung

Für die bei den Finanzämtern erwachsenen Unterlagen, unabhängig von Aufbewahrungsmedium (Papier, Mikrofiche, elektronische Speicherung), hat die Finanzverwaltung bundeseinheitliche „Bestimmungen zur Aufbewahrung und Aussonderung von Schriftgut bei den Finanzämtern“ erlassen. Dabei handelt es sich um Verwaltungsvorschriften.

Die Bestimmungen sehen für die bei den Steuerfahndungs- sowie Bußgeld- und Strafsachenstellen erwachsenen Unterlagen generell eine 10-jährige Aufbewahrungsfrist vor (Nr. 4.3 bzw. 4.5 der Bestimmungen). Diese Aufbewahrungsfrist war bereits mehrfach Gegenstand eines Schriftwechsels mit dem Staatsministerium der Finanzen. Dabei wurde von mir neben der Dauer auch die undifferenzierte Anwendung nur **einer** Frist auf eine Vielzahl von unterschiedlichen Sachverhalten problematisiert. Insbesondere gilt dies für Verfahrenseinstellungen.

Aus datenschutzrechtlicher Sicht besteht folgender Handlungsbedarf:

Die Finanzverwaltung stützt die Datenspeicherung in den in Rede stehenden Sachverhalten insbesondere auf § 88 AO (Untersuchungsgrundsatz), § 208 AO (Aufgaben der Steuerfahndung) und § 386 AO (Zuständigkeit der Finanzbehörde bei Steuerstrafsachen). Die genannten Bestimmungen enthalten Erhebungsbefugnisse, aber keine gesetzliche Regelung für eine Datenspeicherung insbesondere auch keine über deren Dauer. Die eingangs erwähnten Verwaltungsvorschriften können diese Lücke nicht füllen, da ihnen kein Normcharakter zukommt. Einer Rechtsgrundlage bedarf es aber immer, wenn mit der fraglichen Datenverarbeitung ein Eingriff in das informationelle Selbstbestimmungsrecht verbunden ist. Die Rechtsprechung hat dem folgend erst kürzlich festgestellt, dass auch die Aufbewahrungsdauer von (hier) Strafverfahrensakten einer Regelung durch ein formelles, den Grundsätzen des Volkszählungsurteiles entsprechenden Gesetzes bedarf. Das erkennende Oberlandesgericht bezieht seine Entscheidung ausdrücklich auch auf die Aufbewahrung von strafrechtlichen Ermittlungsakten mit Verfahrenseinstellungen nach § 170 StPO (OLG Frankfurt, Beschluss vom 16.08.1998, NJW 1999, S. 73).

Die oben erwähnten Bestimmungen der Abgabenordnung datieren zeitlich vor Erlass des Bundes- und der Landesdatenschutzgesetze sowie vor dem Volkszählungsurteil des Bundesverfas-

sungsgerichts. Der Gesetzgeber ist gehalten, etwa entstandene Regelungslücken zu schließen. Die Fortführung der bisherigen Praxis ohne Einschränkungen kann nur während einer Übergangszeit hingenommen werden.

Bis zum Erlass einer gesetzlichen Regelung ist zwischen dem Interesse an der weiteren Speicherung (soweit diese zur Aufgabenerfüllung der Finanzbehörde noch erforderlich ist) und dem Interesse des Betroffenen an der Beseitigung der Beeinträchtigung, die mit der Speicherung und Nutzung seiner Daten verbunden ist, abzuwägen.

Dies gilt in besonderem Maße für Unterlagen über Steuerpflichtige, bei denen die Steuerfahndungs- bzw. Bußgeld- und Strafsachenstelle die Ermittlungen ergebnislos eingestellt hat. Eine generelle Aufbewahrungsfrist von 10 Jahren, welche nicht auf den Einzelfall abstellt, ist zur Aufgabenerfüllung weder erforderlich noch angemessen. Die für den Justizbereich anzuwendenden Aufbewahrungsbestimmungen stehen für derartige Fälle i.d.R. nur eine 5-jährige Aufbewahrungszeit vor. Für die im länderübergreifenden staatsanwaltschaftlichen Verfahrensregister gespeicherten Datensätze beträgt die Aufbewahrungsdauer sogar nur 2 Jahre (§ 476 Abs. 2 Satz 2 StPO). Es liegt nahe, vergleichbare Fristenregelungen auch im Bereich der Finanzbehörden zu schaffen.

Ich habe mich in diesem Sinne an das Staatsministerium der Finanzen gewandt. Das Staatsministerium vertritt, unter Hinweis auf Erörterungen der AO-Referatsleiter des Bundes und der Länder, die Auffassung, dass sich die Anforderung an die Speicherung und Nutzung von Daten der Finanzämter ausschließlich nach der Abgabenordnung richteten. Die Regelungen des Landesdatenschutzgesetzes seien insoweit nicht anwendbar . Die Unhaltbarkeit dieser Auffassung habe ich oben dargelegt.

Weiterhin wurde mir mitgeteilt, dass sich die Referatsleiter dafür ausgesprochen hätten, dass das Bundesministerium der Finanzen mit dem Bundesbeauftragten für den Datenschutz Gespräche zur Präzisierung der Vorschriften der Abgabenordnung in datenschutzrechtlicher Sicht aufnimmt.

Wenigstens das ist zu begrüßen.

11.5 Führung von Fahrtenbüchern durch Ärzte

Die Frage, ob die Finanzverwaltung für Zwecke der ertragssteuerlichen Behandlung der Nutzung betrieblicher Kraftfahrzeuge für Privatfahrten Ärzte verpflichten kann, in einem Fahrtenbuch Name und Anschrift der aufgesuchten Patienten aufzuführen, wurde zwischen den obersten Finanzbehörden des Bundes und der Länder und den Datenschutzbeauftragten des Bundes und der Länder kontrovers diskutiert.

Ich habe zu der Problematik in meinem 18. Tätigkeitsbericht unter Nr. 11.3 ausführlich Stellung genommen. Ich habe dabei die Auffassung vertreten, dass es Ärzten, als einer der in § 102 Abs. 1 Nr. 3 c AO genannten Berufsgruppe, aufgrund der ihnen obliegenden Verschwiegenheitspflicht verwehrt ist, ein Fahrtenbuch nach den Vorstellungen der Finanzverwaltung zu führen. Das dieser Berufsgruppe aufgrund der genannten Bestimmung der Abgabenordnung eingeräumte Auskunftsverweigerungsrecht umfasst auch Name und Anschrift der behandelten Patienten.

In einem Schreiben des Bundesministeriums der Finanzen vom 23.07.1999 an den Bundesbeauftragten für den Datenschutz, dem Verhandlungen mit dem Bundesbeauftragten für den Datenschutz vorangegangen waren, wurde folgende Regelung getroffen:

Zu Reisezweck, Reiseziel und Reiseroute reicht neben der Angabe des Datums, des Kilometerstands und des Zielorts grundsätzlich die Angabe „Patientenbesuch“ aus, wenn Name und Adresse der Patienten vom Arzt in einem vom Fahrtenbuch getrennt zu führenden Verzeichnis festgehalten werden.

Die Vorlage dieses Verzeichnisses darf nur verlangt werden, wenn tatsächliche Anhaltspunkte vorliegen, die Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen im Fahrtenbuch begründen und die Zweifel anders nicht auszuräumen sind.

Die strittige Frage, ob ein Arzt im Hinblick auf § 102 Abs. 1 Nr. 3 c AO die Bekanntgabe von Namen und Anschrift seiner Patienten in einem Fahrtenbuch verweigern darf, wäre damit letztendlich zwar nicht gelöst, ihre praktische Bedeutung aber deutlich reduziert. Die Entscheidung über die Reichweite von § 102 Abs. 1 Nr. 3 c AO werden letztlich die Gerichte zu treffen haben.

Einige andere Landesbeauftragte für den Datenschutz haben mich über die erfolgte Umsetzung in ihrem jeweiligen Zuständigkeitsbereich in Kenntnis gesetzt.

Inzwischen hat mir das Staatsministerium der Finanzen mitgeteilt, dass es die nachgeordneten Dienstbehörden angewiesen hat, nach dem getroffenen Kompromiss zu verfahren.

11.6 Zugriff der Finanzverwaltung auf Datenverarbeitungssysteme im Rahmen der Außenprüfung

Im Zuge des im Juli 2000 endgültig verabschiedeten Steuersenkungsgesetzes wurde auch eine datenschutzrechtlich relevante Änderung der Abgabenordnung vorgenommen. Der neu eingeführte § 147 Abs. 6 AO eröffnet der Finanzverwaltung im Rahmen einer Außenprüfung künftig die Möglichkeit, das DV-System des zu prüfenden Steuerpflichtigen zu nutzen. Die Finanzverwaltung kann auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden.

Im Rahmen des Gesetzgebungsverfahren konnten in gewissem Umfang datenschutzrechtliche Gesichtspunkte eingebracht werden. Insbesondere ist der ursprünglich von der Finanzverwaltung geforderte Online-Zugriff auf das Rechenwerk des zu prüfenden Steuerpflichtigen entfallen.

Es muss sichergestellt werden, dass die Finanzverwaltung künftig auch auf automatisiert vorgehaltene Buchführungsdaten nur in dem Umfang zugreifen kann, wie ihr dies bei herkömmlichen Unterlagen in Papierform gestattet ist. Probleme ergeben sich dann, wenn Buchführungsdaten mit anderen betrieblichen Daten (bspw. Personaldaten) vermischt gespeichert sind.

Zwar waren und sind die Unternehmen (Steuerpflichtigen) aufgrund § 9 BDSG und auch der vom Bundesministerium der Finanzen erlassenen „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ gehalten, den Datenbestand des Unternehmens gegen unberechtigte Kenntnisnahme zu schützen. Insbesondere muss dabei sichergestellt werden, dass nur berechtigte Personen in dem ihrem Aufgabenbereich entsprechenden Umfang auf Programme und Daten zurückgreifen können. Im Zuge des Gesetzgebungsverfahrens wurde aber deutlich, dass viele Unternehmen bisher keine oder nicht ausreichende Abschottungsmaßnahme ergriffen haben.
Es ist deshalb zu begrüßen, dass die erstmalige Anwendbarkeit der durch § 147 Abs. 6 AO der Finanzverwaltung eingeräumten Möglichkeiten auf den 1. Januar 2002 hinausgeschoben wurde. Dies gibt den Unternehmen Gelegenheit, ihre Datenverarbeitungssysteme mit einer Software auszustatten, welche eine Beschränkung des Zugriffs der Finanzverwaltung auf die steuerlich für die konkrete Außenprüfung relevanten Daten ermöglicht.

11.7 Auskunftsersuchen der Finanzverwaltung über Teilnehmer an Fortbildungsveranstaltungen

Eine Aus- und Fortbildungsstätte für Bedienstete des Öffentlichen Dienstes hat mich um Mitteilung gebeten, ob aus datenschutzrechtlicher Sicht einem Auskunftsersuchen einer Oberfinanzdirektion über Name und Anschrift von Teilnehmern an drei von der Fortbildungsstätte durchgeführten Auslandsfortbildungsveranstaltungen stattgegeben werden kann.

Für Zwecke der Durchführung von Veranstaltungen erhält die Fortbildungsstätte von der Stammdienststelle der zur Fortbildung anstehenden Bediensteten Personal(grund)daten. Diese Daten erlangen bei der Fortbildungsstätte nach meiner Auffassung nicht die Qualität von Personal(akten)daten. Sie haben vielmehr Sachaktenqualität und für ihren Schutz gelten die allgemeinen datenschutzrechtlichen Bestimmungen. Bei Prüfung des eingangs geschilderten Sachverhalts waren deshalb die spezialgesetzlichen Bestimmungen zum Personalaktengeheimnis (Art. 100 ff. BayBG) nicht einzubeziehen. Zum Tragen kommen aber steuerliche Rechtsvorschriften.

Die Oberfinanzdirektion stützt ihr Auskunftsverlangen auf § 93 AO.

Die Finanzbehörden können sich zur Sachaufklärung der Beweismittel bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich halten. Dieses Ermessen hat sich aber an den allgemein gültigen Grenzen der Erforderlichkeit, Verhältnismäßigkeit, Erfüllbarkeit und Zumutbarkeit zu orientieren. Bei Auskunftsersuchen wird die Verhältnismäßigkeit u.a. durch eine im Gesetz vorgesehene Beweismittelreihenfolge berücksichtigt. Nach § 93 Abs. 1 Satz 3 sollen andere Personen (und auch Behörden: hier überschneidet sich die Auskunftspflicht mit der Amtshilfepflicht nach § 111 AO) als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. Der Begriff „sollen“ bedeutet nach herrschender Meinung, daß die Finanzbehörden im Regelfall nach § 93 Abs. 1 Satz 3 AO verfahren müssen und nur in besonders gelagerten atypischen Fällen davon abweichen dürfen. Einen derartigen atypischen Fall hat die Rechtsprechung u.a. bei der Ermittlung von unbekannten Steuerpflichtigen gesehen.

Im vorliegenden Fall werden aber, anders als bei gegenüber den Finanzbehörden verschwiegenen Einnahmen, die Aufwendungen für die Fortbildungsveranstaltung i.d.R. als Werbungskosten im Rahmen der Veranlagung geltend gemacht. Die Finanzbehörden haben also in jedem steuerlich relevanten Fall die Möglichkeit der Prüfung der Zulässigkeit des Werbungskostenabzugs.

Bei der steuerlichen Anerkennung der Aufwendungen von Studienreisen kann ein Kriterium (unter vielen) das Vorliegen eines homogenen Teilnehmerkreises sein (vgl. Abschn. 117 a EStR). Ziel und Zweck des vorliegenden Auskunftsverlangens dürfte allerdings nicht die Prüfung der Abzugsfähigkeit der Aufwendungen in einem Einzelfall sein, sondern, im Hinblick auf die Aufgabe der Finanzverwaltung, die Gleichmäßigkeit der Besteuerung sicherzustellen, die Fertigung von Kontrollmitteilungen an die Wohnsitzfinanzämter der Reiseteilnehmer, soweit bei einem Teilnehmer der Abzug versagt wurde.

Hierzu ist zu bemerken, daß für diese Zwecke mildere Mittel zur Verfügung stehen. Bspw. könnte für eine bestimmte Reise über die Oberfinanzdirektion ein Kontrollhinweis an die nachgeordneten Finanzämter übermittelt werden, mit der Maßgabe, die Aufwendungen für diese bestimmte Reise nicht als Betriebsausgaben/Werbungskosten anzuerkennen.

Meine Rechtsauffassung wird durch ein nach meiner Kenntnis rechtskräftiges Urteil des Finanzgerichts Düsseldorf zu der in Rede stehenden Problematik gestützt. Das Gericht hält ein mit obigem Sachverhalt vergleichbares Auskunftsersuchen (hier gegenüber einer als Veranstalter auftretenden Industrie- und Handelskammer) ebenfalls für nicht zulässig.

Bei Erteilung der Auskunft hält das Gericht darüber hinaus das Vertrauensverhältnis zwischen dem Reiseveranstalter (hier: der IHK) und den Reiseteilnehmern (hier: den von der IHK betreuten Unternehmern) für ernstlich tangiert, was die Durchführung der der IHK obliegenden Aufgaben künftig gefährden würde. Das Auskunftsersuchen wird deshalb auch als für nicht zumutbar erachtet. Auch diese Argumentation kann analog auf den von mir zu beurteilenden Sachverhalt übertragen werden.

11.8 Datenübermittlungen der gemeindlichen Steuerämter an die Religionsgemeinschaften für Zwecke der Erhebung der Kirchengrundsteuer

Immer wieder wenden sich Gemeinden im Zusammenhang mit Anfragen zu Grundstücksdaten durch römisch-katholische bzw. evangelisch-lutherische Kirchensteuerämter an mich. In bestimmtem Umfang besteht Auskunftspflicht.
Bei den geschilderten Anfragen der Kirchensteuerämter handelt es sich um Anfragen an die (Grund-) Steuerämter der Gemeinden. Die Grundsteuermessbeträge unterliegen als Besteuerungsgrundlagen dem Steuergeheimnis (§ 30 Abgabenordnung, AO). Eine zulässige Durchbrechung des Steuergeheimnisses ist u.a. aufgrund der Bestimmung des § 31 Abs. 1 AO möglich. Danach sind Finanzbehörden berechtigt, Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge an Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, zur Festsetzung von Abgaben mitzuteilen. Für Datenübermittlungen aus dem Bereich der gemeindlichen Steuern (Art. 13 KAG) gelten die genannten Bestimmungen der AO entsprechend (§ 1 Abs. 2 Nr. 1 AO i.V. § 111 AO).

Art. 1 des Kirchensteuergesetzes berechtigt Kirchen, Religionsgemeinschaften und weltanschauliche Gemeinschaften, die Körperschaften des öffentlichen Rechts sind, Kirchensteuern zu erheben. Diese können nach dem Maßstab der Grundsteuermessbeträge auch als Kirchengrundsteuer erhoben werden (Art. 1 Abs. 2 Nr. 1 KirchStG). Art. 16 KirchStG ermächtigt die vorgenannten Gemeinschaften zum Zweck der Erhebung von Kirchengrundsteuer eigene Steuerordnungen zu erlassen. Weiterhin wird bestimmt, dass Kirchengrundsteuer nur insoweit erhoben werden darf, als ein Angehöriger der erhebenden Gemeinschaft Eigentümer ist (Art. 16 Abs. 3 KirchStG), und dass Unterlagen, deren die Steuerverbände für die Besteuerung bedürfen, von den zuständigen Staats- und Gemeindebehörden zur Verfügung gestellt werden (Art. 16 Abs. 5 KirchStG).

Die bayerischen (Erz-)Diözesen haben von dieser Ermächtigung des Art. 16 KirchStG Gebrauch gemacht und am22.03.1995 eine Ordnung über die Erhebung von Kirchensteuern in ihrem Bereich erlassen.
Die Evangelisch-Lutherische Landeskirche hat aufgrund der Ermächtigung am 14.02.1967 eine Steuerordnung für die Kirchengrundsteuer in ihrem Bereich erlassen.

Von wesentlicher Bedeutung ist, dass aufgrund der genannten Rechtsgrundlagen umlagepflichtig nur Angehörige der jeweiligen Kirche sind, die Schuldner der Grundsteuer für land- und forstwirtschaftliche Betriebe sind. Sonderregelungen bestehen für konfessions- und glaubensverschiedene Ehen sowie für Miteigentümerschaft.

Auch die Steuerordnungen weisen auf die Mitwirkungspflicht der Staats- und Gemeindebehörden hin. In diesem Zusammenhang wird auch auf die Bekanntmachung des Bayer. Staatsministeriums des Innern vom 09.11.1984 (MABl.S.638) verwiesen, welche die Gemeinden verpflichtet, in bestimmtem Umfang den Religionsgemeinschaften Unterlagen zur Verfügung zu stellen.

Zur Auskunftserteilung benötigen die Grundsteuerstellen die Konfession des Betroffenen. Soweit dieses Datum nicht bereits bei den Grundsteuerstellen bekannt ist, besteht die Möglichkeit, dieses von den Meldebehörden zu erheben. Die Zulässigkeit einer solchen Datenübermittlung aus dem Melderegister innerhalb der Gemeindeverwaltung beurteilt sich nach Art. 31 Abs. 7 Satz 1 MeldeG. Danach ist die Übermittlung der Religionszugehörigkeit an das gemeindliche Steueramt zulässig, da dieses Datum dort zur Auskunftserteilung und damit zur Aufgabenerfüllung erforderlich ist (Art. 31 Abs. 7 Satz 1 i.V.m. Abs. 1 und Art. 3 Abs. 1 Nr. 1, 2, 11 und 12 MeldeG).

11.9 Erhebung des Fremdenverkehrsbeitrags durch gemeindliche Steuerämter

Eine Gemeinde hat sich an mich mit der Frage gewandt, ob es zulässig sei, für Zwecke der Erhebung des Fremdenverkehrsbeitrages die Inhaberin eines Dienstleistungsunternehmens aufzufordern, eine Aufstellung sämtlicher Kunden mit Angabe von Namen, Anschrift und jeweils erzieltem Umsatz vorzulegen. Die Aufstellung sollte dazu dienen, den Vorteil, der der Unternehmerin durch den Fremdenverkehr im Gemeindegebiet erwachsen war, näher zu quantifizieren. Von Seiten der Unternehmerin wurde bestritten, aus dem Fremdenverkehr einen Vorteil zu ziehen. Aus datenschutzrechtlicher Sicht ist zu dem vorgetragenen Sachverhalt Folgendes zu bemerken:

Nach Art. 6 KAG können Gemeinden unter bestimmten Voraussetzungen einen Fremdenverkehrsbeitrag erheben. Die Abgabe bemisst sich nach den besonderen wirtschaftlichen Vorteilen, die dem einzelnen Abgabepflichtigen aus dem Fremdenverkehr erwachsen. Das Bayerische Staatsministerium des Innern hat dazu mit Bekanntmachung vom 28.06.1978 eine Mustersatzung einschließlich näherer Erläuterungen veröffentlicht (vgl. MABl.S.464). Zum wirtschaftlichen Vorteil eines Abgabeschuldners wird ausgeführt, dass dieser sich nicht berechnen lasse und daher geschätzt werden müsse. Dabei sei auf die konkreten Verhältnisse des einzelnen Schuldners und nicht auf vorgegebene Rahmensätze abzustellen.

Diese Vorgaben waren Auslöser der Forderung der Gemeinde an die Dienstleisterin, die genannten Angaben vorzulegen.
Aufgrund von Art. 13 Abs. 1 KAG sind u.a. im Zusammenhang mit der Erhebung des Fremdenverkehrsbeitrags eine Vielzahl von Bestimmungen der Abgabeordnung entsprechend anzuwenden. Von besonderer Bedeutung sind im vorliegenden Sachverhalt die §§ 85 bis 93 AO. Nach § 88 AO ermittelt die Finanzbehörde (hier die Körperschaft, der die Abgabe zusteht), den Sachverhalt von Amts wegen. Sie bestimmt dabei Art und Umfang der Ermittlungen. Die Beteiligten sind zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet (§ 90 AO). Die Beteiligten haben insbesondere die für die Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen (§ 93 AO). Bei einem Auskunftsverlangen – wie hier – ist aber zu beachten, dass es zur Ermittlung eines relevanten Steuer-(hier: Abgabe-)Sachverhalts erforderlich sein muss, es muss weiterhin verhältnismäßig, erfüllbar und zumutbar sein. Insbe-

sondere die Kriterien der Verhältnismäßigkeit und Erfüllbarkeit erscheinen in vorliegendem Sachverhalt fraglich.

Dabei bin ich davon ausgegangen, dass in einem Dienstleistungsunternehmen der in Rede stehenden Art in nicht unerheblichem Umfang sowohl die Dienstleistung selbst, als auch Warenverkäufe gegen Barzahlung getätigt werden. Die angeforderten Daten könnten also in diesen Fällen nur dem Kassenbuch entnommen werden. Eine ordnungsgemäße Kassenbuchführung setzt im Grundsatz die Erfassung jedes einzelne Geschäftsvorfalls voraus. Bei Gewerbetreibenden, die auch Waren oder Dienstleistungen an ihnen nicht bekannte Kunden abgeben, besteht jedoch keine Verpflichtung zur Einzelaufzeichnung. Es genügt hier eine summarische Ermittlung der Tageseinnahmen (Registrierkassenstreifen). Auch wenn im vorliegenden Fall ein Kassenbuch „händisch“ geführt werden sollte, wird in einer Vielzahl von Fällen die Dienstleisterin über die angeforderten Daten nicht verfügen. Dies gilt vor allem in jenen Fällen, in denen Kunden der Unternehmerin nicht bekannt sind, etwa weil es sich um Touristen oder einheimische Gelegenheitskunden handelt. Die Darstellung einer nicht näher qualifizierbaren und quantifizierbaren Teilmenge erscheint aber zur Ermittlung des wirtschaftlichen Vorteils als nicht geeignet.

Unabhängig von diesen mehr in der praktischen Durchführung liegenden Problemen erscheint mir die Anforderung auch unverhältnismäßig. Es muss zu einer Abwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe kommen. Der Belastung des mit der Aufklärung in Anspruch Genommenen ist das zu erwartende Ergebnis gegenüberzustellen. Dabei sind auch etwaige Persönlichkeitsrechte dritter Personen (hier von Kunden) zu berücksichtigen. Die Anforderung erscheint mir insbesondere unter diesem Aspekt als zu weitgehend.

11.10 Weitergabe von gemeindlichen Steuerdaten in einem Zivilverfahren

Im Rahmen einer Eingabe musste ich folgenden Sachverhalt datenschutzrechtlich beurteilen:

Eine bayerische Kommune hat im Zuge eines Zivilverfahrens zum Zwecke der Beweiserhebung neben Auszügen aus dem Melderegister auch Auszüge aus der sog. „gemeindlichen Lohnsteuerliste“ an das zuständige Amtsgericht übermittelt. Nach den Regelungen der Zivilprozessordnung wurden die vorgelegten Unterlagen dort auch den Prozessbeteiligten zugänglich.

Die genannte Lohnsteuer-Liste enthielt neben Namen und Anschrift die Merkmale Geburtsdatum, Steuerklasse, Kinderfreibeträge, Anzahl der zu berücksichtigenden Kinder, Familienstand, Konfessionszugehörigkeit sowie ggf. nach Anweisung des zuständigen Finanzamts einzutragende Pauschbeträge für Behinderte.

Neben den Angaben über die Prozessgegner enthielt die Liste auch vollständige Angaben von 34 weiteren, am Verfahren vollkommen unbeteiligten Bürgern der Kommune. Die Kommune hatte deren Angaben in der weitergegebenen Kopie nicht geschwärzt.

Die Rechtslage stellt sich wie folgt dar:

Aufgrund der Bestimmung des § 39 Abs. 6 Einkommensteuergesetz sind Gemeinden insoweit, als sie Lohnsteuerkarten ausstellen oder Eintragungen auf den Lohnsteuerkarten vornehmen und ändern, örtliche Landesfinanzbehörden. Sie haben dementsprechend das Steuergeheimnis zu wahren (§ 30 i.V.m. § 1 Abgabenordnung).

Eine zulässige Durchbrechung des Steuergeheimnisses ist nur aufgrund § 30 Abs. 4 Nr. 1 – 5, Abs. 5, Abs. 6 Abgabenordnung möglich. Die gesetzliche Regelung ist abschließend.

Für die Offenbarung der Steuerdaten der 34 nicht am Zivilverfahren beteiligten Bürger der Stadt ist eine derartige Offenbarungsbefugnis offensichtlich nicht gegeben.

Aber auch die Offenbarung der steuerlichen Daten der Prozessgegner war nicht befugt. Aus den bereits erwähnten Bestimmungen des § 30 Abs. 4 - 6 Abgabenordnung könnte allenfalls § 30 Abs. 4 Nr. 2 Abgabenordnung in Betracht kommen, der eine zulässige Durchbrechung des Steuergeheimnisses dann ermöglicht, wenn sie durch Gesetz ausdrücklich zugelassen ist. Die hier infrage kommenden Vorschriften der Gemeindeordnung und der Zivilprozessordnung enthalten aber keine derartigen ausdrücklichen Ermächtigungen.

Die Übermittlung des an das Amtsgericht übermittelten Auszugs aus der Lohnsteuerliste der Kommune verstößt damit in erheblichem Umfang gegen datenschutzrechtliche Bestimmungen (hier: § 30 Abgabenordnung).

Ich habe die Datenübermittlung formell aufgrund Art. 31 Abs. 1 BayDSG beanstandet. Der Datenschutzverstoß war nicht geringfügig, sondern erheblich. Er konnte durch die bereits erfolgte Bekanntgabe der Daten an die Verfahrensbeteiligten auch nicht mehr rückgängig gemacht werden.
Das Gewicht des Datenschutzverstoßes wird noch dadurch verstärkt, dass, entgegen der Auffassung der Kommune, die Prozessparteien nicht generell zur Verschwiegenheit verpflichtet sind. Nach einer Akteneinsicht gem. § 299 Abs. 1 Zivilprozessordnung oder aufgrund einer Kenntnisnahme bspw. durch Übersendung von Unterlagen durch den beauftragten Prozessvertreter, sind Dritte, soweit sie nicht dem in § 203 Strafgesetzbuch genannten Personenkreis angehören, nicht gehindert, die erlangten Erkenntnisse weiter zu verbreiten.

12 Personalwesen

12.1 Personalakten

12.1.1 Übertragung der Beihilfesachbearbeitung auf Dritte

Im Berichtszeitraum sind einige Kommunen mit der Frage an mich herangetreten, inwieweit eine Übertragung der Beihilfesachbearbeitung auf außerhalb der Verwaltung des Dienstherrn stehende Dritte zulässig sei. Es wurden sowohl die Möglichkeit kommunaler Zusammenarbeit als auch die Übertragung auf private Stellen (z. B. in Form einer GmbH) angesprochen. Eine Auslagerung der Beihilfesachbearbeitung ist wegen der damit verbundenen Trennung von Personalverwaltung und Beihilfefestsetzung (vgl. 17. Tätigkeitsbericht, Nr. 12.2) einerseits zu begrüßen. Auf der anderen Seite sollte mit der Verlagerung keine Verschlechterung des Datenschutzniveaus bezüglich der Beihilfeunterlagen der Betroffenen verbunden sein.

- Kommunale Zusammenarbeit

  Wird die Beihilfesachbearbeitung von einer Dienststelle einer anderen kommunalen Körperschaft im Rahmen der gesetzlich vorgesehenen kommunalen Zusammenarbeit wahrgenommen, die ja zum Zweck hat, originär getrennte Aufgaben gemeinschaftlich zu erfüllen, stehen beamtenrechtliche Regelungen nicht entgegen, soweit eine Zusammenarbeit nach den kommunalrechtlichen Vorschriften zulässig ist (vgl. Wilde/Ehmann/Niese/Knoblauch, BayDSG, Handb. XIV. 9.d.cc). Durch die Aufgabenübertragung der Beihilfesachbearbeitung durch Zweckvereinbarung auf eine andere Gebietskörperschaft fungiert diese künftig als „Dienststelle“ der bisher zuständigen Kommune (vgl. Art. 12 Abs. 2 i.V.m. Abs. 1 Bayer. Besoldungsgesetz-BayBesG).
  Die Schutzvorschriften für Beihilfeunterlagen gelten hier in vollem Umfang (vgl. die Übertragung der Beihilfesachbearbeitung im staatlichen Bereich auf die Bezirksfinanzdirektionen).

- Beihilfeabrechnung durch private Stellen

  Schon bisher konnten Gemeinden, Gemeindeverbände und sonstige der Aufsicht des Staates

unterstehende Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zur Rückdeckung ihrer Beihilfeverpflichtungen eine Versicherung abschließen (Art. 11 Abs. 2 BayBesG i.d.F.der Bek vom 13. August 1982, BayRS 2032-1-1-F); darunter verstand man auch die Möglichkeit, Beihilfeabrechnungen durch private Versicherungsunternehmen durchführen zu lassen (vgl. Wilde/Ehmann/Niese/Knoblauch, BayDSG, Handb. XIV. 9.d.aa). Eine Übertragung auf sonstige private Stellen war jedoch unzulässig.

Der Gesetzesentwurf der Staatsregierung zur Änderung besoldungsrechtlicher Vorschriften (vgl. hierzu LT-Drs. 14/3980 vom 4. Juli 2000) sieht demgegenüber in § 1 Nr. 6 b eine Ergänzung des Art. 12 Abs. 2 BayBesG dahingehend vor, dass sich die Gemeinden, Gemeindeverbände und sonstigen der Aufsicht des Staates unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zur Erfüllung ihrer Beihilfeverpflichtungen auch „sonstiger geeigneter Stellen“ bedienen und hierzu die erforderlichen Daten übermitteln können. Nach derzeitigem Kenntnisstand soll diese Rechtsänderung zum 1. Januar 2001 in Kraft treten.

Gegen die Erweiterung der Übertragungsmöglichkeit auf sonstige geeignete **private** Stellen, die nicht Versicherungsunternehmen sind, habe ich im Gesetzgebungsverfahren grundsätzliche rechtliche Bedenken erhoben, da der besondere Geheimnisschutz durch die in § 203 Abs. 1 Nr. 6 StGB gesetzlich geregelte Verschwiegenheitspflicht unter anderem nur bei privaten Kranken**versicherungen**, nicht bei sonstigen privaten Stellen gewährleistet ist. Diese institutionelle Verpflichtung bietet einen besseren Schutz für die Beihilfeberechtigten als die aufgrund meiner Einwände in den Gesetzestext (Art. 12 Abs. 2 Satz 2 Halbsatz 2 BayBesG) aufgenommene bloße Pflicht, private Dritte nach dem Verpflichtungsgesetz im Einzelfall persönlich zur Wahrung der Daten zu verpflichten. Meine Forderung - in Anlehnung an Art. 100 d und Art. 100 g BayBG - Regelungen zum Akteneinsichtsrecht der Betroffenen, zur Pflicht zur Aussonderung bzw. Löschung der Daten und zur Rückgabe von Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, in den Gesetzestext aufzunehmen, wodurch eine Verschlechterung des Datenschutzniveaus für die Betroffenen verhindert werden soll, wurde nicht berücksichtigt. In den für private Stellen geltenden Regelungen des Bundesdatenschutzgesetzes ist ein Akteneinsichtsrecht der Betroffenen nicht enthalten. Diese haben somit lediglich ein Auskunftsrecht, das auch nach der geplanten Neufassung des § 34 BDSG

nur besteht, soweit die Daten zumindest in oder aus nicht-automatisierten Dateien verarbeitet werden (vgl. § 27 Abs. 1 BDSG-Entwurf). Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, müssen nach dem BDSG nicht unverzüglich zurückgegeben werden und konkrete Fristen zur Aufbewahrung von Beihilfeunterlagen sind im BDSG nicht vorgesehen. Mein Vorschlag, sämtliche beauftragten Stellen meiner Kontrollbefugnis zu unterwerfen, wurde abgelehnt.

12.1.2 Bekanntgabe von Leistungsstufen, -prämien und -zulagen

Im Vollzug der Leistungsstufenverordnung vom 20. Februar 1998 und der Bayerischen Leistungsprämien- und Leistungszulagenverordnung vom 15. Dezember 1998 sowie der hierzu ergangenen Durchführungshinweise stellte sich bei verschiedenen Anfragen die Frage, inwieweit eine Personalvertretung Einsicht in Listen, die die Namen der Empfänger bei der Vergabe von Leistungsstufen enthält, erhalten darf und ob die Namen der Empfänger von Leistungsprämien innerhalb einer Behörde bekannt gemacht werden dürfen. Ich habe die Auffassung vertreten, dass der Personalrat im Hinblick auf seine gesetzliche Aufgabenstellung einen Anspruch gegenüber dem Dienststellenleiter hat, dass dieser ihm die Namen der Beschäftigten mitteilt, die eine Leistungsstufe erhalten haben oder in einer Stufe verbleiben. Zum Schutz der Empfänger dürfe das allerdings nur in der Weise geschehen, dass lediglich Einblick in entsprechende Unterlagen innerhalb der Dienststelle gewährt wird. Eine Aushändigung hat zu unterbleiben. Die Mitglieder der Personalvertretungen haben über die ihnen bekannt gewordenen Tatsachen Stillschweigen zu bewahren. Gleiches gilt für die Vergabe von Leistungsprämien und Leistungszulagen. Da diese leistungsbezogenen Zahlungen Bestandteil der Bezüge sind, handelt es sich um Personalaktendaten, die nur für Zwecke der Personalverwaltung oder der Personalwirtschaft unter Berücksichtigung des Erforderlichkeitsgrundsatzes verwendet werden dürfen. Eine Bekanntgabe der Namen der Empfänger von Leistungsstufen, -prämien oder -zulagen innerhalb einer Behörde, beispielsweise im internen Mitteilungsblatt, ist daher ohne Einwilligung der Betroffenen unzulässig.

12.1.3 Bekanntgabe von Lohn- und Gehaltsdaten in kommunalen Gremien

Lohn- und Gehaltsberechnungen enthalten personenbezogene Daten, die den Personalakten zuzurechnen sind und besonderen Schutz genießen. Dieser Schutz schränkt nicht nur die Datenübermittlung an Dritte ein, sondern erfordert auch innerhalb einer Behörde Vorkehrungen, die den Kreis derer, die Kenntnis von Daten aus Personalakten erhalten, so klein wie möglich halten. Hieraus folgt, dass den entscheidungsbefugten kommunalen Gremien personenbezogene Daten von Bediensteten und Stellenbewerbern nur in dem Umfang mitgeteilt werden dürfen, wie es zur Behandlung und Beschlussfassung erforderlich ist. Auch die den kommunalen Gremien zugewiesene Überwachungsbefugnis erlaubt keine uneingeschränkte Information über die bei der Gemeinde vorhandenen Unterlagen. Bei einer Beförderung/Höhergruppierung dürften vorwiegend Kriterien wie die Dauer der Wahrnehmung höherwertiger Aufgaben, die Erfüllung der Tätigkeitsmerkmale, das Dienstalter, die beamtenrechtlichen und tarifvertraglichen Voraussetzungen und die Bewährung für die Auswahlentscheidung kommunaler Gremien ausschlaggebend sein. Je nach Art der zu treffenden Entscheidung können noch weitere Angaben über den Betroffenen benötigt werden. Nettolohnberechnungen sind jedoch für die Entscheidung kommunaler Gremien nicht erforderlich und damit unzulässig.

12.1.4 Prüfung der Personalverwaltung einer Universität

Im Zuge der datenschutzrechtlichen Prüfung der Zentralverwaltung und einer Fakultät einer Universität konnte ich feststellen, dass die seit etwa sechs Jahren im Bayerischen Beamtengesetz enthaltenen Regelungen zur Personalaktenführung, die ich für die Beschäftigten des Tarifbereichs wegen der gleichen Interessenlage für analog anwendbar halte, nach wie vor nur zum Teil umgesetzt werden (vgl. 18. Tätigkeitsbericht, Nr. 12.1). Ich habe meine Feststellungen zum Anlass genommen, alle bayerischen Universitäten auf die wesentlichen Grundsätze bei der Personalaktenführung hinzuweisen.
Bei den zur geprüften Fakultät gehörenden Instituten und Einrichtungen werden sowohl Personalneben- als auch Personalteilakten (z.B. Urlaub, Abwesenheit) im Rahmen der jeweiligen personalrechtlichen Befugnisse geführt. Den Personalgrundakt führt die Zentralverwaltung. Scheidet ein Mitarbeiter aus, wird dessen Personalteil-/nebenakt zwar ausgesondert, aber auf unbe-

stimmte Zeit aufbewahrt. Nebenakten (Unterlagen, die **auch** im Grund- bzw. Teilakt vorhanden sein müssten) sind jedoch zu vernichten, sobald sie nicht mehr benötigt werden, spätestens mit dem Ausscheiden des Beschäftigten aus dem aktiven Dienst. Um die Vollständigkeit des Grundakts in jedem Fall sicherzustellen, habe ich empfohlen, die Teil- und Nebenakten ausgeschiedener Mitarbeiter zunächst an die Zentralverwaltung für einen Abgleich des Inhalts zu übermitteln. Bei eventuellen Nachfragen ausgeschiedener Beschäftigter kann die Fakultät auf den bei der Zentralverwaltung aufzubewahrenden Grundakt verweisen. Unabhängig vom Abschluss des Personalakts nach Art. 100 g Abs. 1 BayBG ist zu beachten, dass Unterlagen über Erholungsurlaub, Erkrankungen, Umzugs- und Reisekosten nur noch **fünf Jahre** nach Ablauf des Bearbeitungsjahres aufzubewahren sind. Eine längere Aufbewahrung für Zwecke der Personalverwaltung/-wirtschaft ist nach dieser gesetzlichen Regelung nicht erforderlich. Ich habe die Universität gebeten, die vorhandenen Personalakten sukzessive zu bereinigen.

Soweit bei den einzelnen Stellen der Universität Datenbanken mit Personaldaten (z. B. Personaldatei, Krankheit, Abwesenheit) geführt werden, die aufgrund ihres Umfangs und ihrer Verknüpfungsmöglichkeiten Verfahren zur Personalverwaltung darstellen, ist zu beachten, dass diese der Mitbestimmung der Personalvertretung nach Art. 75 a Abs. 1 Nr. 2 BayPVG, der Regelung des Art. 100 h Abs. 5 BayBG und der Freigabeverpflichtung gemäß Art. 26 BayDSG unterliegen. Die Löschungsfristen richten sich hierbei nach Art. 100 g Abs. 5 i.V.m. Abs. 1 bis 4 BayBG.

12.1.5 Behandlung dienstlicher Rügen und Abmahnungen

Durch eine Eingabe wurde ich darauf aufmerksam, dass in einem Krankenhaus die Abschrift eines Schreibens, das eine dienstliche Rüge enthielt, in einem unverschlossenen Umschlag der Krankenhauspforte zugeleitet worden war. Dort sollte es für die Oberschwester hinterlegt werden. Andere Beschäftigte des Krankenhauses als die Adressatin hatten von dem Inhalt Kenntnis genommen.

Dieses Vorgehen habe ich gem. Art. 31 Abs. 1 Satz 1 BayDSG als datenschutzrechtlichen Verstoß beanstandet. § 9 Abs. 1 Satz 1 BDSG, der gem. Art. 3 Abs. 1 Satz 1 BayDSG in diesem Fall anzuwenden war, sieht vor, dass alle öffentlichen Stellen, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführungen der Vorschriften des BDSG zu gewährleisten.

Erforderlich wäre hier die Zuleitung der Abschrift in einem verschlossenen Umschlag mit dem Namen der Adressatin gewesen, da dadurch selbst bei einem Einlegen in ein falsches Postfach eine Kenntnisnahme durch eine andere Person hätte verhindert werden können. Angesichts des geringen Aufwands und der Sensibilität der in dem Schreiben enthaltenen personenbezogenen Daten, die nicht zur allgemeinen Kenntnisnahme bestimmt waren, wäre dies auch angemessen gewesen.

Weiterhin ist in ähnlichem Zusammenhang in einem anderen Fall die Frage an mich herangetragen worden, ob es aus datenschutzrechtlicher Sicht zulässig sei, auf der Empfangsbestätigung einer Abmahnung den Betreff „Abmahnung“ aufzunehmen. Ich habe mich dahingehend geäußert, dass auch der auf einer Empfangsbestätigung stehende Betreff „Abmahnung“ einen Verstoß gegen § 9 Satz 1 BDSG darstellt. Zwar wurde die Abmahnung in diesem Fall dem Betroffenen – wie erforderlich – in einem verschlossenen Umschlag zugestellt. Trotzdem konnten wegen des Betreffs andere als die zuständigen Personen (z.B. Sachbearbeiter der Personalabteilung) und der Betroffene selbst Kenntnis vom Gegenstand des Schreibens nehmen. Die Empfangsbestätigung hätte z.B. nur den Betreff „Schreiben vom ...“ tragen können. Angesichts der Sensibilität des Datums, das nicht zur allgemeinen Kenntnisnahme bestimmt ist, wäre dies auch angemessen gewesen.

12.1.6 Äußerungen eines Dienstherrn über einen Bediensteten in der Öffentlichkeit

Ein Bediensteter einer Stadt hat sich darüber beschwert, dass sich sein Dienstherr über ihn in öffentlicher Stadtratssitzung und in der Presse in unzulässiger Weise zu seiner Person geäußert habe. Während einer öffentlichen Stadtratssitzung und in einem Leserbrief hatte sich der Bürgermeister zu internen Differenzen zwischen dem Betroffenen und dessen Mitarbeitern und zu Unstimmigkeiten zwischen der Behördenleitung und dem Bediensteten hinsichtlich dessen Amtsführung geäußert. Ich habe das Vorgehen der Stadt im wesentlichen aus folgenden Gründen beanstandet:
Die Ausführungen hinsichtlich interner Differenzen hätten aus Gründen des Persönlichkeitsschutzes allenfalls in nicht-öffentlicher Sitzung erfolgen dürfen. Die öffentliche, negative Beurteilung der Amtsführung des Betroffenen, von der auch die lokale Presse berichtete, verletzt diesen in seinem Recht auf informationelle Selbstbestimmung. Die aus dem Fürsorgeanspruch des Beamten resultierende Verschwiegenheitspflicht des Dienstvorgesetzten gebietet äußerste Zurückhaltung bei beurteilenden Äußerungen bzw. Kritik an der Amtsführung des Bediensteten gegenüber der Öffentlichkeit. Es ist Aufgabe der Vorgesetzten, die pflichtgemäße Amtsführung zu kontrollieren, Verstöße zu beanstanden und ebenso Richtlinien für Ermessens- und Handlungsspielräume vorzugeben. Die Verantwortung nach außen kann es erfordern, dass die Öffentlichkeit über Beanstandungen und Weisungen informiert wird. Soweit die Amtsführung nach außen kritisch gewürdigt wird, kommt jedoch der Einhaltung einer sachlichen Form besondere Bedeutung zu. Die in einem Leserbrief des Bürgermeisters enthaltenen den Betroffenen abwertenden Äußerungen entsprechen dieser Forderung nicht und hätten deshalb unterbleiben müssen.

12.1.7 Behandlung eines Rechnungsprüfungsberichts in öffentlicher Sitzung

Der Verwaltungs- und Personalausschuss einer Stadt beschäftigte sich in öffentlicher Sitzung mit verschiedenen Feststellungen eines Prüfungsberichts des Bayerischen Kommunalen Prüfungsverbands über die städtischen Zulagenregelungen. Eine Feststellung betraf die Eingruppierung sowie die Zahlung von Zulagen und Pauschalen an einen Bediensteten. Der Bericht enthielt zwar nicht dessen Namen, wohl aber seine Funktion als Vorsitzender des Gesamtpersonalrats. Der Bericht war anschließend unter Namensnennung Gegenstand der Berichterstattung in der örtlichen Presse.

Über die Öffentlichkeit oder Nichtöffentlichkeit von Sitzungen des Stadtrats und seiner Ausschüsse ist nach Art. 52 Abs. 2 GO zu entscheiden; demnach sind Sitzungen öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche Einzelner entgegenstehen. Personalangelegenheiten sind danach in der Regel in nicht-öffentlicher Sitzung zu behandeln. Im Bericht war der Name des betroffenen Bediensteten zwar nicht genannt, der Zusammenhang zwischen Funktion und Stelleninhaber war wegen der besonderen Stellung des Betroffenen als Vorsitzender des Gesamtpersonalrats jedoch ohne weiteres herstellbar. Auf diese Weise wurden die im Bericht enthaltenen personenbezogenen Daten wie Höhergruppierung, Zulagen und Rufbereitschaftspauschale bekannt gemacht. Diese sensiblen personenbezogenen Daten sind dem Begriff „Personalangelegenheiten“ zuzuordnen. Die berechtigten Ansprüche des Betroffenen auf Wahrung seiner Privatsphäre waren höher zu werten, als das Informationsinteresse der Öffentlichkeit. Da der Betroffene durch die Bekanntgabe seiner personenbezogenen Daten in seiner privaten und dienstlichen Stellung maßgeblich beeinträchtigt wurde, habe ich die Behandlung des ihn betreffenden Teils des Prüfungsberichts in öffentlicher Sitzung beanstandet.

12.2 Kontrollbefugnisse des Arbeitgebers/Dienstherrn

12.2.1 Postöffnung in Behörden

Mehrere Eingaben und Anfragen veranlassen mich, auf folgende allgemeine Grundsätze der Postöffnung in Behörden hinzuweisen (hinsichtlich verschiedener Einzelfragen verweise ich beispielsweise auf Nr. 8.7 des 16. TB und Nr. 3.5.1 des 17. TB):

Die Öffnung **dienstlicher** Post an Bedienstete und von Bediensteten ist im Rahmen des Direktionsrechts des Dienstvorgesetzten grundsätzlich zulässig. Soweit es sich jedoch erkennbar um Privatpost handelt, ist eine Öffnung unzulässig (Verletzung des Brief- bzw. Postgeheimnisses gem. Art. 10 GG). Nach § 9 Abs. 2 der Allgemeinen Dienstordnung (ADO) für die bayerischen Behörden ist bei Sendungen mit der Behördenanschrift und dem Zusatz „z. Hd. von“ sicherzustellen, dass der bezeichnete Empfänger von ihnen Kenntnis erhält. Im Unterschied hierzu sind Sendungen mit der persönlichen Anschrift – ohne das hierfür eine besondere Kennzeichnung „persönlich“ oder ähnliches notwendig wäre – dem Adressaten ungeöffnet auszuhändigen. Enthalten sie dienstliche Mitteilungen, muss sie der Empfänger unverzüglich an die Eingangsstelle zurückgeben. Darüber hinaus ist in weiteren Fällen aus datenschutzrechtlichen Gründen eine ungeöffnete Weitergabe der Post erforderlich, z. B. an Bedienstete in der Funktion als Personalratsmitglied, als behördlicher Datenschutzbeauftragter oder als Gleichstellungsbeauftragte. Die Behörde hat entsprechende organisatorische Regelungen zu treffen, dass die an diese Stellen direkt adressierten oder entsprechend als vertraulich gekennzeichneten Postsendungen ungeöffnet von der Posteingangsstelle weitergeleitet werden. Auch in Zweifelsfällen sollte die für diese Stellen bestimmte Post unmittelbar zugeleitet werden. Durch § 9 Abs. 1 Satz 3 letzter Halbsatz ADO ist grundsätzlich sichergestellt, dass dienstliche Schreiben, die keinem besonderen Vertrauensschutz unterliegen, an die Posteingangsstelle zurückgegeben und von dort weiter geleitet werden.

12.2.2 Nutzung von Tonbandaufzeichnungen in Rettungsleitstellen

Ein Beschäftigter einer Rettungsleitstelle hat mir vorgetragen, dass seine Dienststelle zur Nachvollziehbarkeit von Einsatzabläufen aufgezeichnete Telefongespräche unbefugt für arbeitsrechtliche Ermittlungen gegen ihn verwendet habe. Ich habe diese Nutzung der Tonbandaufzeichnung als unzulässig angesehen und aus folgenden Gründen beanstandet:
Gemäß Art. 16 Abs. 1 Bayerisches Rettungsdienstgesetz dürfen im Rettungsdienst personenbezogene Daten nur erhoben, aufbewahrt oder genutzt werden, soweit dies zur Ausführung und Abwicklung von Notfallrettung und Krankentransport, zum Nachweis ordnungsgemäßer Ausführung des Einsatzes sowie für die weitere Versorgung des Patienten erforderlich ist oder der Betroffene eingewilligt hat. Nach dem Wortlaut sowie Sinn und Zweck der Vorschrift (Beweissicherung für etwaige aus dem Notfalleinsatz entstehende Zivil- oder Strafverfahren) gehe ich davon aus, dass sich die genannte Vorschrift nicht ausschließlich auf personenbezogene Daten der Notfallpatienten, sondern auch auf die Daten des Einsatzpersonals bezieht. Die Nutzung der Tonbandaufzeichnung erfolgte weder im Zusammenhang mit einem Rettungseinsatz noch mit ausdrücklicher Einwilligung des betroffenen Mitarbeiters, etwa um ihn vor ungerechtfertigten Beschwerden zu schützen.

Auch fehlte die notwendige Beteiligung der zuständigen Personalvertretung für die Einführung und Anwendung der Telefonaufzeichnung als einer technischen Einrichtung zur Überwachung des Verhaltens oder der Leistung der Beschäftigten (vgl. Art. 75 a Abs. 1 Nr. 1 BayPVG). Die Einhaltung der Mitbestimmungsrechte des Personalrats ist jedoch weitere Voraussetzung für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Beschäftigten.

12.3 Rechte der Gleichstellungsbeauftragten

Eine Gleichstellungsbeauftragte hat mich gefragt, inwieweit sie ein Einsichtsrecht in Bewerbungsunterlagen, Bewerberlisten und Personalakten habe. Ich habe zur Klärung des Umfangs des gesetzlich normierten Informationsanspruchs der Gleichstellungsbeauftragten (Art. 18 Abs. 2 und 3 BayGlG) das Staatsministerium der Finanzen und das Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit um fachliche Äußerung gebeten. Im Ergebnis ist unter datenschutzrechtlichen Gesichtspunkten eine Einsichtnahme in den nachfolgend dargestellten Fällen akzeptabel.

Personalakten

Eine Einsichtnahme in Personalakten ist nur mit Zustimmung des Betroffenen zulässig (Art. 18 Abs. 3 Satz 4 BayGlG).

Bewerbungsunterlagen

Das Recht zur umfassenden Einsichtnahme in Bewerbungsunterlagen beschränkt sich auf die in Art. 18 Abs. 3 Satz 2 BayGlG aufgelisteten Fälle der Beteiligung der Gleichstellungsbeauftragten in konkreten Personalangelegenheiten. Danach findet eine Beteiligung der Gleichstellungsbeauftragten nur dann statt, wenn ein entsprechender Antrag der Betroffenen vorliegt oder die Gleichstellungsbeauftragte hinreichende Anhaltspunkte dafür vorträgt, dass die Ziele des Bayerischen Gleichstellungsgesetzes nicht beachtet werden. Die Einschaltung auf eigene Initiative macht zwar ebenfalls eine Unterrichtung erforderlich, die sich aber auf die grundsätzlichen Informationen über die geplante Stellenneubesetzung beschränken kann. Die Einsichtnahme in Bewerbungsunterlagen und Bewerberlisten ist dabei noch nicht erforderlich.

Eine Nichtbeachtung der Ziele des Bayerischen Gleichstellungsgesetzes scheidet im Rahmen der konkreten Auswahl von vornherein aus, wenn sich entweder nur Frauen oder nur Männer um die zu besetzende Stelle beworben haben. In diesen Fällen findet daher keine Beteiligung der Gleichstellungsbeauftragten am Entscheidungsverfahren statt, die eine Einsichtnahme in die Bewerbungsunterlagen und Bewerberlisten beinhaltet.

Eine Beschränkung der Vorlage auf die Bewerber, die in die engere Auswahl einbezogen sind, ist im Bayerischen Gleichstellungsgesetz nicht vorgesehen. Bereits die Zusammenstellung des aussichtsreichsten Bewerberkreises ist nach Auffassung des Finanzministeriums Ergebnis einer Auswahlentscheidung. Schon in diesem Stadium könnten Auswahlkriterien angewandt werden, die sich nicht allein an Eignung, Befähigung und fachlicher Leistung orientieren oder die von Art. 8 BayGlG vorgegebene Zielsetzung unberücksichtigt ließen. Das habe ich auch im Hinblick auf die ausdrücklich geregelte Verschwiegenheitspflicht der Gleichstellungsbeauftragten in Art. 18 Abs. 4 BayGlG akzeptiert.

Bewerberlisten

Eine Offenlegung von Bewerberlisten, die Unterlagen im Sinne von Art. 18 Abs. 2 BayGlG darstellen, erscheint im Falle einer Beteiligung der Gleichstellungsbeauftragten notwendig, um eine sachgerechte Ausübung der Kontrollfunktion zu ermöglichen. Soweit es sich bei diesen Listen lediglich um eine Zusammenfassung der Bewerbungsunterlagen handelt, besteht aufgrund des umfassenden Einsichtsrechts der Gleichstellungsbeauftragten in die Bewerbungsunterlagen für eine Anonymisierung zum Schutz der Interessen der Bewerber kein Bedürfnis. Aber auch für den Fall, dass die Bewerberlisten darüber hinausgehende Angaben enthalten, erscheint eine Anonymisierung im Hinblick auf die Aufgaben der Gleichstellungsbeauftragten nicht sachgerecht. Hierfür muss sie nach Art. 17 Abs. 1 BayGlG die konkrete Einstellungsentscheidung nachvollziehen können. Dazu müssen regelmäßig die in den Bewerberlisten gesammelten Daten konkreten Personen zugeordnet werden können.

12.4 Fragebogen zur Einstellung von Auszubildenden

Bereits in meinem 18. Tätigkeitsbericht (Nr. 12.4) habe ich mich zu einem von der Städtischen Berufsfachschule für Krankenpflege der Landeshauptstadt München in Zusammenarbeit mit einem berufspsychologischen Institut verwendeten Fragebogen zur Bewerberauswahl für Ausbildungsplätze an dieser Schule geäußert. Dieser Fragebogen hatte aufgrund einzelner Fragen zum Intimbereich der Bewerberinnen und Bewerber in der Öffentlichkeit großes Aufsehen erregt.

Ich habe in meiner abschließenden Stellungnahme die Verwendung dieses Fragebogens durch die Städtische Berufsfachschule für Krankenpflege als rechtswidrig angesehen und die Landeshauptstadt München aufgrund folgender Erwägungen gem. Art. 31 Abs. 1 Satz 1 BayDSG beanstandet:

Zwar ist gem. Art. 85 Abs. 1 Satz 1 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) zur Erfüllung der den Schulen zugewiesenen Aufgaben die Erhebung und die Verarbeitung personenbezogener Daten zulässig. Hiervon umfasst sind auch Daten, die im Zusammenhang mit einem Bewerbungsverfahren zur Aufnahme in die Schule stehen. Art. 85 Abs. 1 Satz 2 BayEUG enthält hierzu auch einige Beispiele (z. B. Adressdaten, schulische Daten), die, wie der Wortlaut („insbesondere“) zeigt, nicht abschließend sind. Zulässig ist die Erhebung dieser Daten jedoch nur, soweit sie für die konkrete Aufgabe, d.h. für die Ermittlung geeigneter Bewerber für die Schule **erforderlich** ist.

Um das zu beurteilen, kann auf die Rechtsprechung des Bundesarbeitsgerichts (vgl. z.B. das Urteil vom 22.10.1986, Az.: 5 AZR 660/85) zurückgegriffen werden. Danach lässt der Schutz des Persönlichkeitsrechts (des Arbeitnehmers) nur solche Fragen (des Arbeitgebers) zu, an denen der Arbeitgeber zur Beurteilung der Eignung und Befähigung des Arbeitnehmers ein objektiv gerechtfertigtes Interesse hat. Es ist zwischen Fragen nach dem persönlichen und beruflichen Werdegang und Fragen mit einem direkten Bezug zur Intimsphäre (z.B. Gesundheit, Sexualität) zu unterscheiden. Im letzteren Fall ist ein besonderer Schutz geboten, da die Intimsphäre zum Kernbereich des Rechts auf informationelle Selbstbestimmung gehört, der besonders abgeschottet und nur ausnahmsweise dem Zugriff anderer geöffnet ist.

Meine datenschutzrechtliche Prüfung nach diesen Maßstäben führte dazu, dass zumindest die bereits im 18. Tätigkeitsbericht aufgeführten und eine weitere Frage aus der Intimsphäre der Bewerber(innen) unzulässig waren, da sie eindeutig über das hinausgingen, was für eine ordnungsgemäße Beurteilung der Eignung der Bewerber(innen) unter Berücksichtigung des Rechts auf Achtung ihrer Intimsphäre erforderlich war.

In diesem speziellen Fall kam schließlich noch hinzu, dass die Betroffenen zum Teil erst 17 oder 18 Jahre alt waren, sodass einige Bewerber z.B. durch die Fragen über ihre Sexualität in erhebliche Gewissenskonflikte gebracht worden sein könnten.

Die Datenerhebung war auch nicht aufgrund einer Einwilligung der Betroffenen zulässig (Art. 15 Abs. 1 Nr. 2 BayDSG). Fraglich war bereits, ob überhaupt eine informierte und freiwillige Einwilligung, wie sie von Art. 15 Abs. 1 und 2 BayDSG gefordert wird, vorlag. Auch das Schriftformerfordernis des Art. 15 Abs. 3 BayDSG und die Tatsache, dass es sich bei den Bewerbern teilweise um Minderjährige handelte, habe ich lediglich ergänzend erwähnt. Entscheidend war hier vielmehr, dass die Datenerhebung bezüglich der aufgeführten Fragen unzulässig war. Eine unzulässige Datenerhebung kann hier jedoch auch durch eine Einwilligung nicht „geheilt“ werden. Hierzu habe ich auf die vergleichbare Rechtslage im Arbeitsrecht hingewiesen, wonach das Fragerecht des Arbeitgebers durch Einholung einer Einwilligung des Bewerbers oder Arbeitnehmers nicht wirksam erweitert werden kann. Das würde nämlich dazu führen, dass die zum Schutz des i.d.R. schutzbedürftigen Arbeitnehmers geschaffene arbeitsrechtliche Beschränkung des Fragerechts durch eine Einwilligung unterlaufen würde.
Schließlich habe ich verlangt, dass die Landeshauptstadt München auf das Unkenntlichmachen der beanstandeten Fragen bei dem berufspsychologischen Institut hinwirkt. Die Landeshauptstadt hat mir daraufhin mitgeteilt, dass die beanstandeten Fragen in den Fragebögen unkenntlich gemacht worden seien. Außerdem sei nicht beabsichtigt, ein vergleichbares Verfahren wieder einzuführen. Letzteres halte ich angesichts meiner Beanstandung und der offenkundigen Unzulässigkeit der genannten Fragen für eine Selbstverständlichkeit.

13 Gewerbe und Handwerk

13.1 Weitergabe von Daten aus den Gewerbeanzeigen innerhalb des Landratsamtes

Nach § 1 Abs. 4 Satz 1 der Verordnung zur Durchführung der Gewerbeordnung (GewV) sind die in den §§ 14 und 55 c der Gewerbeordnung (GewO) bezeichneten Anzeigen bei den Gemeinden zu erstatten. Rechtsgrundlage für die Weitergabe der Gewerbeanzeigen an das Landratsamt ist § 14 Abs. 1 Sätze 3 und 4 GewO i.V.m. § 1 Abs. 2 GewV.

Die fallweise Weitergabe von Daten aus den Gewerbeanzeigen an öffentliche Stellen, soweit diese nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, ist in § 14 Abs. 6 GewO geregelt. Nach § 14 Abs. 7 Satz 1 GewO gilt diese Vorschrift für die regelmäßige oder fallweise Weitergabe von Daten innerhalb der Verwaltungseinheit, der die nach § 14 Abs. 1 GewO zuständige Behörde angehört, entsprechend. Wie der Gesetzesbegründung zu entnehmen ist, ist mit Verwaltungseinheit **nur die jeweilige Gemeinde** (bei Stadtstaaten die Bezirksbehörde) gemeint. Das bedeutet, dass für die Weiterleitung von Daten aus den Gewerbeanzeigen innerhalb des Landratsamtes § 14 Abs. 7 GewO nicht herangezogen werden kann. Dieses darf die Gewerbeanzeigen entsprechend der Aufgabenzuweisung in § 1 Abs. 2 GewV nur für Zwecke der Überwachung der Gewerbeausübung nutzen. Im Ergebnis kommt daher eine Nutzung dieser Daten z. B. durch die Stellen für kommunale Wirtschaftsförderung bei den Landratsämtern nicht in Betracht, während sie bei den kreisfreien Städten unter den Voraussetzungen des § 14 Abs. 7 i.V.m. Abs. 6 GewO zulässig ist. Da es keinen sachlichen Grund für diese Differenzierung gibt und Daten aus den Gewerbeanzeigen auch innerhalb des Landratsamtes von anderen als der für die Gewerbeüberwachung zuständigen Stelle benötigt werden, hätte ich keine Bedenken gegen eine Ergänzung des § 14 Abs. 7 GewO mit dem Ziel, die Datenweitergabe auch innerhalb des Landratsamtes unter den in § 14 Abs. 6 GewO genannten Voraussetzungen zu gestatten.

14 Statistik

14.1 EU-Vorhaben einer Volks-, Gebäude- und Wohnungszählung 2001

In meinem 18. Tätigkeitsbericht habe ich unter Nr. 14.1 von dem EU-Vorhaben einer Volks-, Gebäude und Wohnungszählung 2001 berichtet.

Inzwischen ist davon auszugehen, dass die Bereitstellung der Daten durch die Bundesrepublik Deutschland im Rahmen des Zensus 2001 ausschließlich mittels Angaben aus vorhandenen Statistiken erfolgen soll.

Davon unabhängig hat der Bundesminister des Innern den Entwurf eines Gesetzes zur Erprobung eines registergestützten Zensus (Zensus-Testgesetz) vorgelegt. Die Bundesregierung bleibt damit bei ihrer Entscheidung, dass Deutschland aus Kosten- und Akzeptanzgründen künftig keine herkömmliche Vollerhebung – wie zuletzt bei der Volkszählung 1987 – mehr durchführen wird. Es soll vielmehr ein Methodenwechsel von der Befragung aller Einwohner hin zu einem registergestützten Zensus erfolgen. Der vorliegende Entwurf eines Zensus-Testgesetzes soll die rechtliche Grundlage bilden für Tests, in denen neue Verfahren erprobt und weiterentwickelt werden, immer im Hinblick auf den angestrebten Methodenwechsel.

Ich habe zu dem vorliegenden Gesetzesentwurf zu einzelnen Teilbereichen datenschutzrechtliche Bedenken erhoben bzw. Klarstellungen gefordert (Entstehen eines zentralen bundesweiten Melderegisters beim Statistischen Bundesamt, Rückfluss von Statistikdaten in den Verwaltungsvollzug), denen sich auch das Staatsministerium des Innern angeschlossen hat. Es bleibt der weitere Fortgang des Gesetzgebungsverfahrens abzuwarten.

14.2 Datenerhebung für den 2. Versorgungsbericht der Bundesregierung

Für den 2. Versorgungsbericht der Bundesregierung wird derzeit vom Bundesministerium des Innern eine als Geschäftsstatistik bezeichnete Erhebung veranlasst, die eine bundesweite anonymisierte Meldung von Krankheitsdaten von vorzeitig in den Ruhestand versetzten Beamten an das Bundesministerium vorsieht. Aus datenschutzrechtlicher Sicht bestehen Bedenken, ob eine ausreichende Rechtsgrundlage für die Erhebung vorliegt. Weitere Bedenken bestehen bezüglich der Sicherstellung einer ausreichenden Anonymisierung.
Um eine Geschäftsstatistik handelt es sich nach den üblichen Definitionen dann, wenn Daten, die bei öffentlichen Stellen im Rahmen des Verwaltungsvollzugs erhoben oder angefallen sind, statistisch aufbereitet werden. Eine Geschäftsstatistik kann deshalb von der datenerhebenden/datenspeichernden Stelle bzw. deren übergeordneten Dienstbehörden bis hin zur obersten Dienstbehörde angeordnet werden. Im vorliegenden Fall sollen jedoch von einer obersten Bundesbehörde, welche in keinerlei Hinsicht - bezogen auf die betroffenen Landesbeamten - in den Verwaltungsvollzug eingebunden ist, statistische Daten erhoben und aufbereitet werden.
Es handelt sich somit nicht um eine Geschäftsstatistik, sondern vielmehr um eine amtliche Statistik, deren Anordnung einer gesetzlichen Grundlage bedarf.

Bei der geplanten aktuellen Erhebung werden des Weiteren auch Daten bei den gutachterlich tätigen Amtsärzten erhoben. Diese Datenerhebung erfolgt in jedem Fall außerhalb einer Geschäftsstatistik.

Eine zulässige Geschäftsstatistik müsste sich hingegen auf die bei der datenerhebenden/datenspeichernden Stelle vorhandenen Daten beschränken, die von dieser Stelle ausgewertet und so zusammengestellt werden müssten, dass Rückschlüsse auf einzelne Betroffene zuverlässig ausgeschlossen sind. Die derartig zusammengestellten Ergebnisse könnten dann, ohne dass datenschutzrechtliche bzw. statistikrechtliche Belange berührt wären, an das Bundesministerium des Innern weitergeleitet werden.

Ich sehe meine Rechtsauffassung auch dadurch bestätigt, dass in der Vergangenheit für die Erhebung der Angaben für den 1. Versorgungsbericht mit § 7 Finanz- und Personalstatistikgesetz eine bereichsspezifische Rechtsgrundlage geschaffen wurde.

Ich habe mich in diesem Sinne an das für statistikrechtliche Fragen zuständige Staatsministerium des Innern gewandt. Das Staatsministerium teilt meine Rechtsauffassung.

Unabhängig von der aufgeworfenen statistikrechtlichen Problematik kann bei der beabsichtigten Erhebung in Einzelfällen auch eine Deanonymisierung mit einem gewissen Zusatzwissen nicht zuverlässig ausgeschlossen werden.

Dieser Personenbezug ist bspw. denkbar in Bereichen mit geringen Betroffenenzahlen (z. B. Richter).
Denkbar ist auch, dass den für statistische Zwecke übermittelten Unterlagen noch der Versandumschlag mit der Absendeangabe der jeweiligen Dienststelle oder auch ein Begleitschreiben beiliegt. Gleiches gilt für einen Hinweis auf den ggf. für eine bestimmte Dienststelle zuständigen begutachtenden Amtsarzt.

Je nach Größe der Dienststelle wäre der Datensatz mit geringem Zusatzwissen einem bestimmten Beschäftigten zuzuordnen.

Ich habe mich aufgrund dieser Sachlage an das für Personalaktenrecht federführende Staatsministerium der Finanzen mit der Bitte gewandt, die Übermittlung der Daten an das Bundesministerium des Innern zunächst auszusetzen.

Eine Lösungsmöglichkeit der Problematik sehe ich in meinem Vorschlag, die benötigten Daten bei der datenerhebenden/datenspeichernden Stelle auszuwerten und so zusammenzustellen, dass Rückschlüsse auf einzelne Betroffene nicht möglich sind. Ergänzend ist darauf hinzuweisen, dass aufgrund Art. 6 Abs. 1 BayStatG mit der Durchführung von Geschäftsstatistiken auch das Landesamt für Statistik und Datenverarbeitung beauftragt werden kann.

Das Staatsministerium der Finanzen hat mir inzwischen mitgeteilt, dass es die Übermittlung der Erhebungsvordrucke vorerst ausgesetzt hat. Es hat mir weiterhin den Entwurf für eine bereichsspezifische Ermächtigungsgrundlage für die Datenerhebung und –übermittlung, die im Beamtenversorgungsgesetz eingefügt werden soll, übermittelt. Gegen den Gesetzesentwurf bestehen in

seiner augenblicklichen Fassung wegen fehlender Bestimmtheit datenschutzrechtliche Bedenken. Die Diskussion mit dem Staatsministerium ist insoweit noch nicht abgeschlossen.

15 Schulen und Hochschulen

15.1 Veröffentlichungen in einer Homepage und im Jahresbericht einer Schule

Im 18. Tätigkeitsbericht habe ich mich unter Nr. 15.1 mit der Frage befasst, unter welchen Voraussetzungen Lehrerdaten und Daten der Elternbeiratsmitglieder einer Schule im Internet veröffentlicht werden dürfen. Aufgrund vieler Anfragen von Schulen weise ich nochmals darauf hin, dass im Hinblick auf die enge lokale Begrenzung des Aufgaben- und Wirkungsbereichs von Schulen das Persönlichkeitsrecht der Schüler, Eltern, Lehrer und des sonstigen Schulpersonals Vorrang vor dem Informationsinteresse einer breiteren Öffentlichkeit (Internetnutzer) hat. Vor der Einstellung personenbezogener Daten ins Internet ist daher die Einwilligung der Betroffenen einzuholen. Bei minderjährigen Schülern, die bereits die entsprechende Einsichtsfähigkeit besitzen (ab etwa 15 Jahren), bedarf es deren Einwilligung, im übrigen der Einwilligung der Erziehungsberechtigten. Die Einholung der Einwilligung hat so zu erfolgen, dass sich die Betroffenen nicht einem Gruppendruck ausgesetzt fühlen. Sie sind dabei darauf hinzuweisen, dass sich ins Internet eingestellte Erreichbarkeitsdaten in der Regel problemlos auslesen lassen und damit nachteilige Auswirkungen verbunden sein können. Das Staatsministerium für Unterricht und Kultus hat Hinweise zu Veröffentlichungen der Schulen im Internet in die überarbeiteten „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ eingefügt, die bereits im Entwurf vorliegen.

Weiterhin häufen sich die Anfragen dazu, inwiefern Fotografien, die Schüler oder andere Personen abbilden (Klassenfotos etc.), auf der Homepage oder auch im Jahresbericht einer Schule datenschutzrechtlich zulässig sind; die bisherigen „Erläuternden Hinweise“ (Stand 1996) äußern sich dazu nicht. Datenschutzrechtlich ist hierzu festzustellen, dass es sich bei Veröffentlichungen, die Schüler oder andere Personen auf der Homepage oder im Jahresbericht einer Schule abbilden, um Datenübermittlungen an Dritte handelt, die nur aufgrund der Einwilligung der Betroffenen zulässig sind (vgl. Art. 15 Abs. 1 BayDSG), da die Voraussetzungen des Art. 85 Abs. 1 BayEUG nicht erfüllt sind. Dies gilt auch dann, wenn den Fotos Namenslisten oder sonstige Namensangaben nicht hinzugefügt sind; denn auch in diesen Fällen sind die auf den Fotos abgebildeten Personen für jeden Betrachter identifizierbar, die dadurch übermittelten Daten also personenbeziehbar (vgl. Art. 4 Abs. 1 BayDSG).

Für den Jahresbericht einer Schule gibt es zwar in Art. 85 Abs. 3 BayEUG eine ausdrückliche Rechtsgrundlage. Zu dem schon danach zulässigen Inhalt eines Jahresberichts sind jedoch Fotos nicht zu zählen. Angesichts des engen Adressatenkreises eines Jahresberichts sehe ich es hier allerdings als ausreichend an, wenn die Betroffenen zu Beginn eines jeden Schuljahres hinreichend deutlich darüber informiert werden, dass Fotos in den Jahresbericht aufgenommen werden sollen und ihnen die Möglichkeit eines Widerspruchs eingeräumt wird. Sofern nur einzelne auf einem Foto abgebildete Personen von ihrem Widerspruchsrecht Gebrauch machen, können diese dann in geeigneter Form unkenntlich gemacht werden. Rein vorsorglich weise ich darauf hin, dass ich eine grundsätzlich denkbare Änderung des Art. 85 Abs. 3 BayEUG nicht für sachgerecht halte, da es tatsächlich den Betroffenen überlassen bleiben sollte, ob sie mit einer Abbildung ihrer Person auf einem Foto im Jahresbericht einer Schule einverstanden sind.

Für Fotos, die Schüler oder andere Personen abbilden, auf der Homepage einer Schule oder auch für die Weitergabe der Fotos an die (lokale) Presse gibt es keine normative Rechtsgrundlage. Hier kann auf eine ausdrückliche Einwilligung der Betroffenen, die vorher auch über die besonderen Risiken einer solchen Veröffentlichung zu informieren sind, nicht verzichtet werden; sollten die Bilder auf der Homepage erneuert werden, ist zudem eine einzelfallbezogene neue Einwilligung notwendig. Hier sollte angesichts der besonderen Risiken für die Persönlichkeitsrechte der Betroffenen erst recht keine Rechtsgrundlage geschaffen werden, um deren Einwilligung entbehrlich zu machen.

15.2 Fragebogenaktionen

Eine Erziehungsberechtigte hat mir vorgetragen, dass bei der an einer Hauptschule durchgeführten Fragebogenaktion zum Thema „Soziales Lernen“ die Anonymität der befragten Schüler nicht gewährleistet gewesen sei und die Eltern nicht ausreichend über den Inhalt der Befragung informiert worden seien. Weiterhin konnte ich feststellen, dass das zur Anonymisierung gewählte Kodierungsverfahren (Nummerierung nach Klassenlisten) nicht sicherstellte, dass die ausgefüllten Fragebogen nicht mehr den einzelnen Schülern zugeordnet werden können.

Für eine ausreichende Elterninformation wäre eine vorherige umfassende Darstellung von Sinn und Zweck des Projekts und der weiteren Datenverarbeitung (was geschieht mit den Daten, wie lange besteht der Personenbezug, Löschung, Veröffentlichung, Inhalt des vorgesehenen Kodierungsverfahrens; vgl. hierzu Nr. 2.3.1 dieses Berichts) notwendig gewesen. Die zu der Fragebogenaktion vorab verteilten Elternbriefe, mit denen die Eltern nach Auffassung der Projektleitung ihre Einwilligung erklärt haben sollen, erfüllten diese Voraussetzungen nicht und bezeichneten die Fragebogenaktion zudem nicht zutreffend als anonym. Von einer informierten Einwilligung als Voraussetzung einer zulässigen Datenerhebung im Sinne des Datenschutzrechts konnte damit nicht ausgegangen werden.

Als mangelhaft habe ich auch den Umstand erachtet, dass die Lehrkräfte die ausgefüllten Fragebogen, die sehr in die persönliche Sphäre hinreichende Fragen zum familiären Umfeld des Kindes enthielten, zumindest teilweise offen eingesammelt haben. Um eine Kenntnisnahme der Lehrkräfte über den Inhalt auszuschließen, hätten die Schüler dazu angehalten werden sollen, die Fragebogen selbst einzukuvertieren. Die Fragebogen wurden zwar in den Fällen, bei denen die Eltern ihre Einwilligung zurückgezogen hatten, vernichtet. Wegen der aufzeigten schwerwiegenden Mängel bei der Durchführung der Befragung habe ich die Fragebogenaktion gleichwohl beanstandet.

15.3 Schülerliste zur Untersuchung bei einem HNO-Arzt

Durch einen Hinweis erfuhr ich, dass ein Förderzentrum für Hörgeschädigte nach einer freiwilligen Gehöruntersuchung künftiger Grundschüler die (zukünftige) Schule und die Eltern der untersuchten und positiv befundenen Kinder über sämtliche Kinder mit einem positiven Befund informierte. Die Information erfolgte mittels einer Liste, auf der sich die Namen dieser (sieben) Kinder, ihre Geburtsdaten und ihre medizinischen Daten (Ergebnisse der Hörabstandsmessung, des Tonaudiogramms und der Tympanometrie) befanden.

Ich habe die Schule auf folgendes hingewiesen:

- Zum einen war die Übermittlung dieser Liste an die Schule durch das den freiwilligen Gehörtest durchführende Förderzentrum nicht zulässig, da dadurch die ärztliche Schweigepflicht unzulässig durchbrochen wurde. Eine solche Durchbrechung wäre nur zulässig beim Vorliegen einer Offenbarungsbefugnis oder –pflicht. Eine solche Befugnis wäre hier die freiwillige und informierte Einwilligung der gesetzlichen Vertreter des jeweiligen Kindes gewesen, die jedoch nicht eingeholt wurde. Sollten Eltern in diese Datenübermittlung nicht einwilligen, dürfte **nur ihnen** das Untersuchungsergebnis **ihres** Kindes bekannt gegeben werden.
- Außerdem war es unzulässig, den betroffenen Erziehungsberechtigten durch die Liste personenbezogene Daten anderer Kinder mitzuteilen. Es ist daher in Zukunft eine entsprechende individuelle Benachrichtigung der Eltern zu gewährleisten

15.4 Evaluation der Lehre

Bereits vor der Verabschiedung des Gesetzes vom 24. Juli 1998 (GVBl S. 443), mit dem das Bayerische Hochschulgesetz in wesentlichen Punkten geändert wurde, habe ich gegenüber dem Staatsministerium für Wissenschaft, Forschung und Kunst zum Ausdruck gebracht, dass ich der Evaluation der Lehre im Hinblick auf die Befragung der Studierenden zurückhaltend gegenüberstehe und unter anderem die Verwertbarkeit der Befragungsergebnisse für nicht unproblematisch halte. Da verschiedene - erst im weiteren Gesetzgebungsverfahren eingearbeitete - Änderungen gegenüber dem ursprünglichen Gesetzentwurf gewisse Rechtsunsicherheiten bewirken, habe ich das Ministerium gebeten, für die Hochschulen erläuternde Hinweise bekannt zu machen. Die Verwendung der im Rahmen der Evaluation ausgewerteten Ergebnisse studentischer Befragungen (vgl. Art. 39 a Abs. 3 Sätze 4 bis 6 BayHSchG) wurde mit mir abgestimmt und wie folgt beschränkt:

Die Bezeichnung der Lehrveranstaltungen, die Namen der Lehrenden und die ausgewerteten Ergebnisse der studentischen Befragungen über Ablauf sowie Art und Weise der Darbietung des Lehrstoffs werden dem Fachbereichsrat und der Leitung der Hochschule bekannt gegeben und zur Bewertung der Lehre verwendet. Demgegenüber werden den Mitgliedern des Fachbereichs, die nicht dem Fachbereichsrat angehören, nur die wesentlichen Ergebnisse der Befragung, ggf. unter Hinzufügung der Stellungnahme des betroffenen Lehrenden, zugänglich gemacht. Die wesentlichen Ergebnisse der Befragung müssen in einer Form zugänglich gemacht werden, die eine Kenntnisnahme durch Personen, die nicht Mitglieder des Fachbereichs sind, ausschließt. Eine Bekanntgabe der Ergebnisse am „schwarzen Brett“ der Hochschule oder gar im Internet wäre daher unzulässig.

Im Lehrbericht, dessen Veröffentlichung keiner Beschränkung unterliegt, dürfen studentische Bewertungen der Lehrenden nicht unter Angabe der Bezeichnung der Lehrveranstaltungen und der Namen der Lehrenden dargestellt werden.

16 Medien

16.1 Pressepapier des Kreisverwaltungsreferenten der LHSt. München zu „Mehmet“

Aufgrund einer Eingabe habe ich das 11-seitige Pressepapier des (ehemaligen) Kreisverwaltungsreferenten der Landeshauptstadt München vom 29.04.1998 zur Ausweisung „Mehmets“ datenschutzrechtlich bewertet. Unter dem Pseudonym „Mehmet“ wird in diesem Pressepapier mit Einzelangaben u.a. die familiäre Ausgangssituation „Mehmets“ geschildert. Gewalt- und Straftaten „Mehmets“ im öffentlichen Bereich, z.B. in Schulen und an U-Bahn-Haltestellen werden unterschiedlich detailliert dargestellt. Berichtet wird auch über „Mehmets“ Fehlverhalten in der Schule und über sonstige Verfehlungen, verbunden mit im Einzelnen ausgeführten elterlichen Versäumnissen zur Begründung, warum zusammen mit dem Aufenthalt „Mehmets“ auch der Aufenthalt seiner Eltern in Deutschland beendet werden sollte. Veröffentlicht werden in diesem Papier auch einzelne Informationen, die dem Kreisverwaltungsreferat (KVR) aus dem Bereich des Stadtjugendamts München zur Verfügung gestellt wurden. Das KVR reagierte mit diesem Pressepapier nicht auf eine Anfrage der Presse, sondern kommentierte damit seine Ausweisungsverfügung vom selben Tage. Im weiteren Verlauf veröffentlichte die Presse Auszüge aus dem KVR-Pressepapier und die Identität des jungen Türken und seiner Familie waren trotz des verwendeten Pseudonyms „Mehmet“ nach kurzer Zeit öffentlich bekannt.

Auf dieses Pressepapier finden die Datenschutzvorschriften Anwendung, da der Presse und Öffentlichkeit nicht ausschließlich anonymisierte, sondern lediglich pseudonymisierte Daten übermittelt wurden. Die über die Presse weitergeleiteten Einzelangaben des KVR-Pressepapiers mit einer Vielzahl von Details über Straftaten, den schulischen und sozialen Werdegang und das gesellschaftliche Umfeld „Mehmets“ konnten nämlich jeweils durch eine Vielzahl von Personen wie bspw. Freunde, Nachbarn, Lehrer, Mitschüler und Eltern usw. relativ unschwer der tatsächlichen Identität „Mehmets“ zugeordnet werden. Wer „Mehmet“ anhand eines solchen Einzelvorgangs identifizieren konnte, erfuhr eine ganze Reihe weiterer Informationen über den ihm nunmehr namentlich bekannten Jugendlichen. Einiges spricht auch dafür, dass die Angaben aufgrund ihrer Detailliertheit angesichts der Möglichkeiten der Presse bereits auch für diese personenbeziehbar waren.

Die Datenübermittlung musste für die Aufgabenerfüllung des KVR erforderlich und somit auch verhältnismäßig gewesen sein. Abzuwägen war also zwischen der Eingriffstiefe in Bezug auf den Betroffenen einerseits und dem Nutzen für die Behörde andererseits. Die Eingriffstiefe in Richtung des Betroffenen durfte gegenüber dem Nutzen für die Behörde nicht außer Verhältnis stehen. Weiter war zwischen einem berechtigten Interesse des Empfängerkreises, der „Mehmet“ aufgrund der detaillierten Angaben im Pressepapier identifizieren konnte, sowie der Presse an der Datenübermittlung und dem schutzwürdigen Interesse des Betroffenen am Ausschluss der Übermittlung abzuwägen. Auf der einen Seite war also auf das Behördeninteresse, vermuteten Angriffen wegen ihrer Linie in der Durchführung des Ausländergesetzes entgegenzutreten sowie auf die Frage eines berechtigten Interesses der Presse und Öffentlichkeit an der Berichterstattung abzustellen. Gegenüberzustellen und dabei abzuwägen war das von der Rechtsordnung geschützte Interesse des zum Zeitpunkt der Presseveröffentlichung noch nicht 14-jährigen, also eines Kindes im Rechtssinn, daran, dass detaillierte personenbezogene Angaben über sein Verhalten nicht von einer breiten Öffentlichkeit zur Kenntnis genommen werden. Zu bedenken war, dass über Ermittlungsergebnisse der Polizei grundsätzlich nur in anonymisierter Form berichtet werden darf. Das Gleiche gilt für die Pressearbeit der Justiz. Auch ein Straftäter muss es regelmäßig nicht hinnehmen, dass über ihn vor der Hauptverhandlung für einen großen Empfängerkreis personenbeziehbar über sein gesamtes strafrechtlich relevantes Vorleben berichtet wird. Die Abwägung zwischen Aufgaben der Behörde und dem Interesse des Betroffenen verbietet es in der Regel umso mehr, dass personenbeziehbar **rein vorsorglich** über beabsichtigte Verwaltungsmaßnahmen berichtet wird, insbesondere wenn der Betroffene zu einer solchen Berichterstattung nicht durch Angriffe auf die Behörde Anlass gegeben hat. Angaben aus polizeilichen Ermittlungsergebnissen, noch dazu rein vorsorglich, halte ich deshalb für höchst problematisch. Zu weit gehend und unzulässig ist jedenfalls die detaillierte Berichterstattung über einen zum Veröffentlichungszeitpunkt noch nicht 14-jährigen: Die Rechtsordnung stellt Jugendliche, insbesondere aber Kinder im Rechtssinn unter ihren besonderen Schutz. § 48 Abs. 1 Jugendgerichtsgesetz bestimmt die Nichtöffentlichkeit von Verhandlungen gegen Jugendliche einschließlich der Entscheidungsverkündung. Der BGH führt in seiner Rechtsprechung hierzu aus, die Tendenz des JGG gehe dahin, „im Verfahren vor den Jugendgerichten die Gedanken der Erziehung und des Schutzes der Jugend dem Prinzip der Öffentlichkeit der Hauptverhandlung überzuordnen [...]. Dem jungen Angeklagten soll die bei öffentlicher Verhandlung und Verurteilung drohende Bloß-

stellung mit den daraus erwachsenden Nachteilen für seine persönliche, soziale und berufliche Entwicklung erspart bleiben [...]“ (NJW 1998, S. 2066).

Mit der detaillierten Angabe der polizeilichen Ermittlungsergebnisse über „Mehmet“ erfolgte eine derartige Bloßstellung. Diese ins Einzelne gehende Darstellung hätte wegen ihrer Vergleichbarkeit mit der Erörterung der Einzelheiten der Tatbegehungen in einer mündlichen Verhandlung gegen einen Jugendlichen nicht veröffentlicht werden dürfen.

Damit wurde durch diese detaillierte Darstellung das Gebot der Verhältnismäßigkeit verletzt. Auch ein „berechtigtes Interesse der Öffentlichkeit“ an einer personenbeziehbaren Darstellung aller Einzelheiten des Vorlebens „Mehmets“ in strafrechtlicher, familiärer und sozialer Hinsicht vor Erlass einer Verwaltungsmaßnahme war bei Abwägung mit den o.a. Interessen des unter 14-jährigen nicht gegeben. Dies gilt trotz der Erwägung, dass „Mehmet“ im Hinblick auf seine Verhaltensweisen und die darüber bereits erfolgte Berichterstattung in den Medien inzwischen zu einer „relativen Person der Zeitgeschichte“ geworden war, für die grundsätzlich ein erhöhtes Interesse der Öffentlichkeit anzuerkennen ist. Da es aber selbst bei einem Erwachsenen fraglich wäre, ob ein solches erhöhtes Interesse eine rein vorsorgliche Informationsübermittlung an die Presse in diesem Umfang rechtfertigen würde, kann dieses Interesse der Öffentlichkeit bei einem Kind nicht dem durch die Rechtsordnung anerkannten erhöhten Schutz vor Bloßstellung vorgehen, da dieser Schutz sonst obsolet würde. Das Pressepapier des KVR verstieß deshalb gegen das Gebot der Verhältnismäßigkeit und der sachgerechten Abwägung.

Des Weiteren enthielt das KVR-Pressepapier auch personenbeziehbare Informationen aus dem Bereich des Stadtjugendamts der LHSt. München, u.a. zur Darstellung (fehlgeschlagener) Versuche verschiedener Personen und Stellen, „Mehmet“ positiv zu beeinflussen. Solche Angaben unterliegen deshalb gem. § 78 Abs. 1 SGB X weiterhin dem Schutz des Sozialgeheimnisses, weshalb das KVR diese Informationen nur zu dem Zweck weitergeben durfte, zu dem sie ihm befugt übermittelt worden waren. Das KVR hatte im Pressepapier verwendete Sozialdaten aus dem Bereich des Jugendamts zur Bearbeitung und Entscheidung des ausländerrechtlichen Verwaltungsvorgangs betreffend „Mehmet“ bzw. zur Erfüllung der Aufgaben der Ausländerbehörde erhalten. Nun darf man zwar grundsätzlich auch die Öffentlichkeitsarbeit des KVR als Aufgabe der Ausländerbehörde ansehen. Eine Nicht-SGB-Stelle wie das KVR ist dabei aber gem. § 78

Abs. 1 S. 1 und 2 SGB X zur Veröffentlichung von Sozialdaten nur insoweit befugt, als auch die Sozialbehörde, aus deren Bereich die Sozialdaten stammen, selbst Öffentlichkeitsarbeit damit betreiben dürfte. Das Stadtjugendamt wäre hierzu **nicht** berechtigt gewesen. Nach § 69 Abs. 1 Nr. 3 SGB X ist die Übermittlung von Sozialdaten nämlich nur zulässig, soweit sie erforderlich ist für die Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verfahren über die Erbringung von Sozialleistungen; die Übermittlung bedarf der vorherigen Genehmigung der zuständigen obersten Bundes- oder Landesbehörde. Der Gesetzgeber hat in § 69 Abs. 1 Nr. 3 SGB X die Zulässigkeit der Öffentlichkeitsarbeit mit Sozialdaten über die Erbringung von Sozialleistungen konkret und abschließend geregelt. Er hat dabei eine einschränkende Sonderregelung zu der allgemein gefassten Übermittlungsbefugnis nach § 69 Abs. 1. Nr. 1 SGB X („zur Aufgabenerfüllung der SGB-Stelle“) getroffen und hat die Zulässigkeit der Öffentlichkeitsarbeit mit Sozialdaten an die vorherige Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde gekoppelt, obwohl diese Befugnis ohnehin nur eingreift, wenn **der Betroffene** die öffentliche Richtigstellung **seiner** unwahren Tatsachenbehauptungen verursacht hat. Keine der Voraussetzungen nach § 69 Abs. 1 Nr. 3 SGB X lag im Fall „Mehmets“ vor. Da auch eine sonstige Übermittlungsbefugnis nach dem SGB nicht in Betracht kam und sich auch und gerade eine Nicht-SGB-Stelle wie das KVR wegen § 78 Abs. 1 SGB X an die Beschränkungen durch das Sozialgeheimnis zu halten hat, konnte es auch unter ausländerrechtlichen Gesichtspunkten keinesfalls befugt sein, von sich aus im Vorfeld einer Medienberichterstattung über die Ausweisung „Mehmets“ und seiner Eltern Öffentlichkeitsarbeit unter Verwendung von Sozialdaten zu betreiben.

Ich habe von einer Beanstandung der LHSt. München im Rahmen des mir eingeräumten Ermessens gem. Art. 31 Abs. 3 BayDSG abgesehen. Die Stadtspitze hatte das Vorgehen des KVR nicht gebilligt, so dass keine Wiederholungsgefahr hinsichtlich eines derart detaillierten und vorsorglichen behördlichen Pressepapiers über ein Kind zu befürchten ist.

17 Technischer und organisatorischer Bereich

17.1 Grundsatzthemen

17.1.1 Ende der Kryptodebatte - Kryptografie als Standard

In den Abschnitten 19.1.4 und 19.1.5 meines 18. Tätigkeitsberichts von 1998 habe ich mich zum Einsatz kryptografischer Verfahren und zur Kryptodebatte (Kryptokontroverse) geäußert und die Notwendigkeit der Anwendung von kryptografischen Methoden zur Sicherung von Datenübertragungen und Datenspeicherungen hervorgehoben.
Mit dem Papier „Eckpunkte der deutschen Kryptopolitik“ vom 02.06.1999 hat nun die Bundesregierung ein klares Votum zugunsten der Anwendung kryptografischer Verfahren und gegen eine momentane Kryptoregulierung abgegeben und die Kryptodebatte damit vorläufig beendet. Insbesondere sind damit die bis dahin bestehenden Bedenken und Unsicherheiten bei Herstellern und Anwendern über die Entwicklung und über evtl. zukünftige Rechtsvorschriften ausgeräumt. Für eine abwartende Haltung besteht somit kein Grund mehr.

Ausgehend von der Erklärung der Bundesregierung haben die Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 58. Konferenz vom 07./08.10.1999 eine entsprechende Entschließung mit dem Titel „Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung“ gefasst. Der vollständige Text der Entschließung ist als Anlage 12 beigefügt und ist auch auf meiner Home-Page veröffentlicht.

Besonders hervorheben möchte ich an dieser Stelle den vorletzten Absatz der Entschließung:
„Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptografischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptografie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.“

Im Rahmen meiner Beratungstätigkeit habe ich in der Vergangenheit immer wieder darauf hingewiesen, dass gem. Art. 7 Abs. 2 Ziff. 9 BayDSG über offene oder öffentliche Netze übertrage-

ne personenbezogene Daten vor unbefugter Kenntnisnahme, vor unbefugtem Kopieren und vor unbefugter Veränderung zu schützen sind. Nur durch die Anwendung kryptografischer Methoden (digitale Signatur und Verschlüsselung) kann dieser Forderung hinreichend Rechnung getragen werden.

Zu häufig ist noch die Haltung verbreitet, die Anwendung kryptografischer Verfahren sei nur entsprechend aufwendig und kompliziert zu behandeln, und deshalb wird sie gerne als Ausnahmefall betrachtet. Dabei wird leider übersehen, dass durch standardmäßige Anwendung kryptografischer Verfahren, insbesondere wenn sie auf Hardwarefunktionalitäten basieren, diese vermeintliche Kompliziertheit erheblich reduziert, die Benutzerfreundlichkeit erhöht, aber auch den Grundforderungen nach Wahrung von Vertraulichkeit, Integrität und Authentizität Rechnung getragen werden kann. Vor allem würde auch in diesem essenziellen und rasant zunehmenden Teilaspekt der Datenverarbeitung das bisher in anderen Bereichen erreichte Niveau von Datenschutz und Datensicherheit nachhaltig gesteigert werden. Gleichwohl sind durchaus vereinzelt positive Initiativen vorhanden, wie z.B. das Projekt „Verdiensterhebung über das Internet“ des Bayerischen Landesamtes für Statistik und Datenverarbeitung (siehe Abschnitt 17.3.10) oder das Projekt „ELSTER“ der bayerischen Steuerverwaltung (siehe Abschnitt 19.3.12 meines 18. Tätigkeitsberichts) zeigen.

Ich wiederhole daher an dieser Stelle meine seit Jahren erhobene Forderung, kryptografische Verfahren standardmäßig einzusetzen und nur im begründeten Ausnahmefall von deren Anwendung abzusehen.

Auch die Datenschutzbeauftragten des Bundes und der Länder verwenden im Übrigen seit Herbst 2000 zur Absicherung ihrer elektronischen Kommunikation untereinander kryptografische Verfahren – obwohl dabei i.d.R. keine personenbezogenen Daten übertragen werden. Ich selbst biete bereits seit 22.02.1999 auf meiner Home-Page meinen öffentlichen PGP-Schlüssel für die sichere E-Mail-Kommunikation mit mir an.

17.1.2 Bayerisches Behördennetz

Am 05.03.1996 und am 07.05.1996 beschloss der Ministerrat die Einführung des Bayerischen Behördennetzes (BYBN). Funktionale Hauptelemente des BYBN sollen die elektronische Kommunikation der angeschlossenen Behörden mittels E-Mail, die Abwicklung von Dialog-Verfahren im Client-Server-Betrieb und sonstige Datenübertragung zwischen Dienststellen sein. Mit den Fragen der Sicherheit und Sicherheitsorganisation im BYBN sind mehrere Gremien und Einrichtungen befasst, die sich aus Vertretern der Bayerischen Staatskanzlei, der Bayerischen Staatsministerien und des Landesamtes für Statistik und Datenverarbeitung (LfStaD) zusammensetzen. Keines dieser Gremien und Einrichtungen kann jedoch für alle Ressorts verbindliche Festlegungen treffen oder gar solche durchsetzen.

Seit Beginn der Arbeiten am BYBN habe ich in den o.a. Gremien wiederholt meine Grundforderungen nach Sicherstellung einer vertraulichen, authentischen und nicht manipulierbaren Datenübertragung durch Anwendung kryptografischer Verfahren (Datenverschlüsselung, Signatur) erhoben. Dabei habe ich meine Bereitschaft bekundet, bis zur Verfügbarkeit von langfristig tragenden Lösungen auch Übergangslösungen zu akzeptieren.

E-Mail

Die ersten beiden Jahre der Sicherheitsdiskussion im BYBN (von März 1996 bis März 1998) waren bestimmt von der Diskussion bzgl. des zu verwendenden E-Mail-Protokolls (X.400 versus SMTP) und der Sicherheitsprotokolle (PEM und S/MIME). Eine von mir angeregte Übergangslösung mit PGP wurde unter Hinweis auf eine bevorstehende, umfassende und dauerhafte Lösung im Rahmen von BASILIKA nicht verfolgt.

Das dritte und vierte Jahr im BYBN (April 1998 bis April 2000) waren geprägt von Tests verschiedener S/MIME-Clients und von deren Interoperabilitätstests. Eine Übergangslösung für sichere E-Mail mit PGP oder mit S/MIME-Clients (mit kurzen Schlüssellängen), die zwar von einigen Gremien beschlossen worden war, wurde aber auch in diesem Zeitraum nicht realisiert. Die ab dem II. Quartal 2000 vorgesehene Verwendung von S/MIME-Clients mit starker Verschlüsselung (Outlook 2000 und TrustedMIME i.V.m. Outlook 98) wurde ebenfalls nicht flächendeckend umgesetzt.

Mitte 2000 wurde auf Empfehlung des zentralen CERT festgelegt, dass übergangsweise - für spezielle Anforderungen - PGP auf Ebene der jeweiligen Poststellen der an das BYBN angeschlossenen Behörden einzuführen sei. Im Übrigen wurde festgelegt, dass eine Zertifizierungsinfrastruktur mit einer vom LfStaD betriebenen Zertifizierungsstelle als Basis für eine zügig zu realisierende Sicherheitslösung aufzubauen sei, wobei die Staatskanzlei und die Staatsministerien bis zum 30.09.2000 sog. Beglaubigungsstellen einrichten sollten. Dieses ist noch nicht erfolgt. Möglichst bis zum 31.12.2000 sollten die Beglaubigungsstellen sodann durch Registrierungsstellen ersetzt werden. Bis dahin sollten für den Austausch sicherer E-Mail auch S/MIME-Clients im erforderlichen Umfang installiert werden.

Zertifizierungsinfrastruktur (PKI, Public Key Infrastructure)

Im September 1997 wurde festgelegt, dass ein X.500-konformes Verzeichnis der Kommunikationsadressen im BYBN aufgebaut werden solle. Produktauswahl und Einrichtung des Verzeichnisdienstes sowie die Errichtung einer Zertifizierungsstelle beim LfStaD erstreckten sich bis Oktober 1999. Zwei Registrierungsstellen - beim LfStaD selbst sowie beim StMI - nahmen Anfang Februar 2000 ihren Betrieb auf.

Die im Dezember 1999 im BYBN veröffentlichten Entwürfe der Regelwerke (Sicherheitsrichtlinien der Zertifizierungsstelle, Antragswesen, Antragsformulare, u.ä.) für die PKI wurden im August 2000 zuletzt aktualisiert, aber bisher von keinem Gremium für verbindlich erklärt.
Meine ablehnende Haltung gegenüber der gewünschten zentralen Erzeugung von PGP-Schlüsseln bei der Zertifizierungsstelle habe ich Mitte 2000 im Unterarbeitskreis Sicherheit dargestellt. Eine zentrale Erzeugung ist nicht erforderlich (jedes Schlüsselpaar kann vom Nutzer selbst erzeugt werden). Die dann erforderliche sichere Übermittlung des Schlüsselpaares an den Nutzer wäre sehr aufwendig. Im Übrigen wäre nicht sichergestellt, dass der private Schlüssel nicht noch in Kopie bei der Zertifizierungsstelle verbliebe. Ich sehe darin ein nicht hinzunehmendes Sicherheitsrisiko.

Im April 2000 wurde angeregt, den Active Directory Service (ADS) von Microsoft anstelle des bisherigen, auf OPEN-LDAP basierenden Systems des LfStaD zu verwenden - das bisher vom LfStaD entwickelte formale Antragswesen für die Erteilung von Zertifikaten solle jedoch aus organisatorischen Gründen beibehalten werden. Die daraufhin geschaffene Projektgruppe „Ein-

satz von Active Directory“ arbeitet seither an der Klärung grundlegender, ressortübergreifender Fragen. Die Klärung dieser Fragen wird m.E. weitere geraume Zeit in Anspruch nehmen.

Das StMLU hat – basierend auf der Empfehlung des zentralen CERT von Mitte 2000 - zwischenzeitlich eine Zertifizierungsstelle für PGP-Keys und einen entsprechenden Key-Server im BYBN in Betrieb genommen.

Sonstige Sicherheitsaspekte

Ein Grundsatz im BYBN ist, dass sich die Teilnehmer gegenseitig vertrauen. Wie schnell dieser Grundsatz infrage gestellt werden kann bzw. muss, ist am Beispiel des auch im BYBN über E-Mail verbreiteten Love-Letter-Wurms von Mitte des Jahres 2000 erkennbar. Als Folgerung aus den gemachten Erfahrungen soll nun beim LfStaD eine zentrale Sicherheitsschleuse eingerichtet werden, die die Absicherung des gesamten E-Mail- und auch Webverkehrs (Aktive Inhalte) in das und aus dem BYBN gewährleisten soll. Dabei ist zurzeit heftig umstritten, wie restriktiv diese zentrale Sicherheitsschleuse eingestellt werden kann und soll, da diese Einstellungen unmittelbaren Einfluss auf Komfort und Möglichkeiten bei der Nutzung des Internet im BYBN nehmen. Die Sicherheit des BYBN muss aber m.E. allen Komfortwünschen vorgehen – entgegen evtl. vorhandener Gegenstimmen.

Diese zentrale Sicherheitsschleuse ist jedoch nur ein Baustein in einem generell erforderlichen Sicherheits- und Notfallkonzept. Da auch diese zentrale Schleuse nicht allen Risiken entgegenwirken kann, sind weitere verfeinernde Maßnahmen auf der Ebene der jeweiligen Ressort- und Teilnetze des BYBN, auf der Ebene des jeweiligen Arbeitsplatzes, im organisatorischen Bereich und ganz besonders durch den einzelnen Endanwender der IuK-Technik notwendig.

Zusammenfassung

Nach nahezu fünf Jahren steht nun eine Zertifizierungsstelle im LfStaD für S/MIME-basierte Zertifikate und ein PGP-Key-Server im StMLU zur Verfügung. Es sind Beschlüsse zur Einrichtung einer Public-Key-Infrastruktur und zur Ausstattung der Dienststellen mit S/MIME-Clients und PGP gefasst, wobei aber die vereinbarten Termine bereits teils nicht eingehalten, teils infrage gestellt werden. Die Regelwerke für die PKI liegen im Entwurf vor. Das Ziel, rasch einen flächendeckenden sicheren E-Mail-Verkehr im BYBN zu gewährleisten, ist demnach nach wie

vor nicht erreicht. Bei all den Anstrengungen um sichere E-Mail darf jedoch auch die sichere Abwicklung von Dialogverfahren im Client-Server-Betrieb und sonstiger Datenübertragungen zwischen Dienststellen nicht vergessen werden.

Aufgrund der bisherigen Erfahrungen habe ich Bedenken, dass sich in nächster Zukunft die Situation bzgl. einer flächendeckenden Sicherheit im BYBN deutlich verbessern wird. Es sind zwar große Anstrengungen bei der Produktauswahl für sichere E-Mail unternommen und auch in jüngster Vergangenheit wieder grundlegende Beschlüsse gefasst worden, aber deren praktische und zeitnahe Umsetzung muss erst noch tatsächlich vollzogen werden. Dabei erscheint mir, dass die ausgesprochen heterogene technische und personelle Ausstattung der BYBN-Teilnehmer sowie die jeweiligen wirtschaftlichen Möglichkeiten bei all den wegweisenden Beschlüssen nicht immer ausreichend berücksichtigt werden. Weitere grundlegende Fragen der Sicherheit (z.B. zentrale Sicherheitsschleuse) i.V.m. Komforteinbußen sind ebenfalls noch nicht abschließend geklärt.

Ein weiterer wesentlicher Grund für meine Skepsis ist auch die Vielzahl an Gremien, von denen aber keines über die entsprechende Möglichkeit verfügt, Sicherheitsvorgaben für alle Bereiche der bayerischen Verwaltung über Ressortgrenzen hinweg bindend festzulegen und auch durchzusetzen.

Ich wiederhole meine Forderung nach umgehender Sicherstellung einer vertraulichen, authentischen und nicht manipulierbaren Datenübertragung im BYBN.

17.1.3 Data Warehouse und Data Mining

Mit zunehmendem Verbreitungsgrad und zunehmender Leistungsfähigkeit der Informations- und Kommunikationstechnik nimmt auch der Umfang der gespeicherten Daten permanent zu. Diese Daten sind in operativen, zentralen oder auch dezentralen Systemen gespeichert, welche einem klar umrissenen und abgegrenzten Zweck dienen und dafür optimiert sind. Die Abfrage- und Auswertemöglichkeiten des jeweiligen Datenbestandes sind in der Regel entsprechend dem Zweckbindungsprinzip ebenfalls auf vordefinierte Zwecke begrenzt und damit relativ eingeschränkt. Das Zweckbindungsprinzip stellt eines der fundamentalen Datenschutzprinzipien dar - jeder soll auch wissen, zu welchem Zweck seine Daten verarbeitet werden. Ad hoc-Abfragen oder gar eine Verknüpfung von Daten verschiedener operativer Systeme zur abstrakteren und auch zur umfassenderen Informationsgewinnung sind ohne die Mithilfe von Statistikern und EDV-Fachleuten nicht ohne weiteres möglich und datenschutzrechtlich nur unter der Voraussetzung einer zulässigen Zweckänderung möglich.

Grundlage von Data Warehouses (DWH) sind die verschiedenen operativen Datenbestände. Mit Hilfe entsprechender Werkzeuge werden diese Rohdatenstrukturen analysiert, Daten selektiert und für die Zusammenführung und eine auf andere Art und Weise strukturierte Speicherung im DWH vorbereitet. Mit den Werkzeugen des Data Mining (DM) werden die scheinbar zusammenhanglosen Daten des DWH nach bisher unbekannten Zusammenhängen durchsucht, wobei neue, ggf. abstraktere aber auch ggf. umfassendere Informationen gewonnen und ggf. auch gespeichert werden sollen.

Die durch die Einrichtung von DWH auf Basis personenbezogener Daten entstehenden potenziellen Risiken für das Recht auf informationelle Selbstbestimmung und für den Schutz auf Privatheit, insbesondere die Verletzung des Zweckbindungsprinzips, sind offenkundig: z.B. Bildung von Persönlichkeitsprofilen, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen und zu lange Datenspeicherung. Ein DWH, das datenschutzfreundliche Technologien verwendet und z.B. nur mit anonymisierten oder pseudonymisierten Daten arbeitet, birgt geringere Risiken. Ein DWH, das ausschließlich mit hinreichend anonymisierten Daten arbeitet und bei dem auch durch die Verknüpfung von anonymisierten Daten eine Reidentifizierung von Einzelpersonen unmöglich ist, ist datenschutzrechtlich unbedenklich.

Im öffentlichen Bereich sind derzeit nur vereinzelt Ansätze und Bemühungen in diese Richtung festzustellen (z.B. sind in Bayern Überlegungen und Bemühungen zur Schaffung eines DWH im Bereich des Staatsministeriums der Finanzen bzgl. der Personalplanung und Stellenbewirtschaftung vorhanden). Gegenwärtig sind verschiedene Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder damit befasst, sich mit dem Themenkomplex auseinander zu setzen und ggf. eine Orientierungshilfe zu erarbeiten, die Hinweise zum datenschutzgerechten Betrieb von DWH geben und eine rechtliche Bewertung derartiger Konzepte ermöglichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder haben bei ihrer 59. Konferenz vom 14./15.03.2000 eine Entschließung zu „Data Warehouse, Data Mining und Datenschutz“ gefasst, in der u.a. die Beachtung des Zweckbindungsprinzips angemahnt wird und die Hersteller und Anwender zur Nutzung von Programmen aufrufen, die die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung möglichst vermeiden. Diese Entschließung ist als Anlage 19 beigefügt und auch auf meiner Home-Page abrufbar.

17.1.4 Prüfkriterien für datenschutzfreundliche Produkte (Common Criteria)

Im Abschnitt 19.1.2 meines 18. Tätigkeitsberichtes habe ich die wachsende Bedeutung von Sicherheitszertifikaten hervorgehoben, bin auf die aktuellen Probleme bei der Zertifizierung von Sicherheitsprodukten eingegangen und habe Maßnahmen aufgezeigt, um aus dem derzeitigen Dilemma herauszufinden.

Ein weiterer Schritt dazu erfolgte 1998 auf internationaler Ebene (verschiedene Länder Europas sowie Nordamerikas) mit der Schaffung der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Common Criteria Version 2.0 (CC)“. Bei den Common Criteria handelt es sich um eine Weiterentwicklung und Harmonisierung der europäischen „Information Technology Security Evaluation Criteria (ITSEC)“ von 1991, der US-amerikanischen „Trusted Computer Security Evaluation Criteria (TCSEC, Orange Book)“ von 1983 und der kanadischen „The Canadian Trusted Computer Product Evaluation Criteria V3.0e (CTCPEC)“ von 1993.

Für den Datenschutz sind die Common Criteria von besonderer Bedeutung, weil erstmals Anforderungen zum Schutz der Privatsphäre in einem derartigen Kriterienkatalog enthalten sind. Dabei sind Grundsätze zur Anonymität, Pseudonymität, Unverkettbarkeit und Unbeobachtbarkeit im Teil „Funktionale Sicherheitsanforderungen - Datenschutz“ enthalten. Mit Hilfe der in den Common Criteria beschriebenen „Protection Profiles“ (PP, Schutzprofile) ist es möglich, unter anderem auch datenschutzspezifische Anforderungen für bestimmte Produkttypen zu definieren. Die Schutzprofile bieten somit für die Anwender von IuK-Technik und für sonstige Bedarfsträger die Möglichkeit, ihre Bedürfnisse zur IT-Sicherheit sowohl den Herstellern als auch den Zertifizierungsstellen gegenüber deutlich zum Ausdruck zu bringen - unabhängig von existierenden Produkten. Dadurch können international vergleichbare und prüffähige Vorgaben für die Entwicklung datenschutzfreundlicher Produkte gemacht werden.

Die Datenschutzbeauftragten von Bund und Ländern möchten die Möglichkeit nutzen, auf Basis der Common Criteria bereits im Vorfeld von Produktentwicklungen solche Schutzprofile zu erstellen, die wesentliche datenschutzrechtliche Anforderungen widerspiegeln. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftrag-

ten von Bund und Ländern hat zu diesem Zweck eine Arbeitsgruppe unter meiner Federführung gebildet, die zunächst ein Schutzprofil zu den Aspekten Verschlüsselung und Pseudonymisierung erstellen soll. Damit könnten beispielsweise eine zugriffssichere Datenspeicherung, eine gesicherte und vertrauliche Datenübertragung innerhalb von lokalen Netzwerken, aber auch über offene und öffentliche Netzwerke sowie eine datenschutzgerechte Erzeugung von Pseudonymen und ggf. Depseudonymisierung mit einem einzigen Sicherheitsprodukt realisiert werden. Konkret könnte mit dem Schutzprofil beispielsweise eine wichtige Voraussetzung geschaffen werden, um die Forderungen der Gesundheitsreform 2000 zur Datenübermittlung der Leistungserbringer an die Krankenkassen datenschutzgerecht umzusetzen.

Das BSI, als der deutsche Vertreter bei der Entwicklung der Common Criteria, ist Mitglied der Arbeitsgruppe. Der erste Entwurf des Schutzprofils zum Thema Pseudonymisierung und Verschlüsselung liegt mit den beschreibenden Teilen vor. Über den Fortgang der Schutzprofil-Entwicklung, in die weitere Experten einzubinden sein werden, werde ich berichten.

17.1.5 Viren im Internet

Durch das alleinige Lesen einer E-Mail wurde ein Computer bisher noch nicht infiziert, was sich allerdings spätestens seit dem Auftreten der Script-Viren (z. B. „I love you“) geändert hat. Diese in einer Script-Sprache wie Visual Basic geschriebenen Würmer (Würmer sind eigenständige Programme, die kein sogenanntes Wirtsprogramm benötigen und sich durch Reproduktion ihres Codes selbständig innerhalb eines Netzes ausbreiten können) können sich in Anhängen von E-Mails verstecken. Wird nun dieser Anhang mit einem Doppelklick gestartet und befinden sich Script-Interpreter wie z. B. die Microsoft-Komponenten Outlook (ab Version 98) oder WSH (Windows Scripting Host - standardmäßig ab Windows 98) im Einsatz, kann der Virus seine Schadensfunktion ausüben.

Ein Anhang (Attachment) einer E-Mail kann aber auch sonstige ausführbare Programme, eine selbstextrahierende Datei oder einen Makrocode (z. B. zur Ausführung in Word-Dokumenten) mit Schadensfunktion enthalten. Diese Anhänge können ebenfalls bei einem Öffnen des Attachments mit Doppelklick den Rechner mit einen Virus verseuchen. Dateianhänge an E-Mails, gleich welcher Art (ob DOC-, VBS-, BAT- oder EXE-Files usw.) und unabhängig von ihrer

Herkunft (aus dem Internet oder aus dem Behördennetz), sollten daher keinesfalls sofort mit Doppelklick geöffnet werden. Stattdessen sollte jeder Dateianhang mit der Funktion „Speichern unter“ auf eine mittels Virenscanner überwachten lokalen Festplatte in einem speziell dafür angelegen Verzeichnis gespeichert werden. Erst dann darf der Dateianhang von der Festplatte aus mit der entsprechenden Anwendung gestartet werden.

Um sich als Outlook-Benutzer soweit wie möglich gegen einen Virenbefall zu schützen, sollte außerdem die Sicherheitsstufe im Internet Explorer über das Menü „Ansicht/(Internet)Optionen/Sicherheit“ auf „Hoch (am sichersten)“ eingestellt sein. Allerdings kann der Internet Explorer bei dieser Einstellung generell keine Visual-Basic-Scripts mehr verarbeiten, was zu Fehlermeldungen beim Internet-Surfen führen kann.

Außerdem sollte darauf geachtet werden, dass die Dateinamenserweiterungen im Windows Explorer angezeigt werden (einstellbar unter *Ansicht/Optionen*). Diese Einstellung gilt dann gleichzeitig für die Anzeige von Dateianhängen in E-Mails.

Desweiteren sollten die Anwender hinsichtlich der Beachtung des Outlook-Warnfeldes beim Öffnen eines Attachments geschult werden. Dieses Dialogfeld ist in den aktuellen Versionen von Outlook integriert und weist darauf hin,

> „dass Webseiten, ausführbare Dateien und andere Anlagen Viren oder Skripts enthalten können, die den Computer beschädigen können. Es ist deshalb wichtig sicherzustellen, dass die Quelle der Datei vertrauenswürdig ist.“

Gleichzeitig wird abgefragt, was mit der Datei passieren soll (Öffnen oder - wie empfohlen - auf Datenträger speichern. Die Deaktivierung dieser Option „Vor dem Öffnen dieses Dateityps immer bestätigen“ sollte per Dienstanweisung verboten werden.
Eine weitere Möglichkeit besteht darin, am zentralen Mail-Server in allen eingehenden E-Mails bei Dateianhängen, die z. B. die Programmendung „.vbs“ oder „.exe“ enthalten, den Punkt beispielsweise durch das Zeichen "~" zu ersetzen. Aus xxx.exe wird dann xxx~exe, bzw. xxx~vbs. Als Alternative dazu kann auch dem Datennamen eine weitere Endung hinzugefügt werden (z. B. test.exe.xxx). Beides bewirkt, dass die Anlage nicht mehr mit Doppelklick aus Outlook gestartet werden kann, sondern zuerst gespeichert und umbenannt werden muss. Die Liste der Dateianhänge kann natürlich nach Bedarf erweitert werden. Diese Maßnahme wurde unter anderem

vom Zentralen Cert (Computer Emergency Respone Team = Einrichtung, die die Verbesserung der Sicherheit von DV-Systemen zum Ziel hat) für das Bayerische Behördennetz ergriffen.

Eine weitere empfehlenswerte Maßnahme besteht darin, ein so genanntes „Dateiblocking“ durchzuführen. Dabei werden Dateianhänge in E-Mails nicht nur auf Viren überprüft, sondern auch bestimmte, einstellbare Dateitypen in so genannten „Quarantäneordner“ abgelegt und nicht an den eigentlichen Empfänger der E-Mail weitergeleitet. Der vorgesehene Empfänger erhält statt des geblockten Dateianhangs einen entsprechenden Hinweis. Möchte der Adressat nun die geblockte Datei, muss er sich an den Systemverwalter (oder eine damit beauftragte Person) wenden. Dieser hat nun die Möglichkeit, entweder diese benannte Datei per E-Mail weiterzuleiten oder direkt in ein benanntes Dateiverzeichnis einzuspeichern.

Unbedingt geblockt werden sollten folgende Dateitypen:

- ausführbare Dateien (wie com, exe, bat)
- in Script-Sprachen erstellte Dateien (z. B. vbs)
- Systemdateien (wie drv, ole, reg, scr, sys)

Die Liste der geblockten Dateitypen ist natürlich jederzeit erweiterbar und neuen Gefahrenquellen anpassbar.
Zur Vermeidung eines Virenbefalls und einer Verunsicherung der Anwender sollte alles, was aus dem Internet kommt, also beispielsweise E-Mails, Download-Dateien, Java-Scripts und ActiveX-Controls, automatisch von Virenscannern überprüft werden. Dabei müssen spezielle Virenscanner zum Einsatz gelangen, die auch Hostile Applets (siehe TZ. 19.3.8 im 18. Tätigkeitsbericht von 1998) aufspüren können. Werden Dateien verschlüsselt übertragen, müssen diese nach dem Entschlüsseln erneut gescannt werden. Der Einsatz von aktuellen Virenscannern sowohl beim zentralen Datenbankserver als auch beim E-Mail-Server und bei der Firewall ist daher unverzichtbar. Auch ein laufendes Scannen der Arbeitsplatzrechner wird angeraten, insbesondere wenn diese PC mit Disketten- und/oder CD-ROM-Laufwerken ausgestattet sind. Da täglich ca. 20 neue Viren auftauchen, bieten Antivirenprogramme nur dann einen größtmöglichen Schutz, wenn sie ständig aktualisiert werden. Ein Restrisiko für einen Virenbefall wird aber bei dieser Flut von neuen Viren immer bestehen.

17.2 Prüfungen, Beratungen und Informationen

17.2.1 Beanstandungen

Die Kontrolle der technischen und organisatorischen Datensicherheitsmaßnahmen war wiederum einer der Schwerpunkte im Berichtszeitraum. Leider habe ich dabei bei zwei Kliniken so schwer wiegende Verstöße gegen den Datenschutz und die Datensicherheit festgestellt, dass ich sie gemäß Art. 31 BayDSG förmlich beanstanden musste. Dabei handelte es sich um folgende Verstöße:

Verschwinden von Patientenakten und Zimmerschlüssel

Bei einer psychiatrischen Klinik wurde festgestellt, dass sowohl aus dem Zimmer eines der Leitenden Oberärzte als auch aus einem anderen Raum, in dem Akten der Sexualtherapie offen gelagert waren und zu dem viele Ärzte und Schwestern ungehinderten Zutritt hatten, Akten verschwunden waren. Außerdem wurde einer Oberärztin der Gruppenschlüssel entwendet. Dieser Schlüssel diente zum Abschließen aller Eingangstüren und aller verschließbaren Behältnisse im Bereich der Oberärzte der Psychiatrie. Zusätzlich wurde festgestellt, dass die Aus- und Rückgabe von Schlüsseln im Bereich der Psychiatrischen Klinik nicht revisionsfähig erfolgte. So wurde es von der Klinikumsleitung geduldet, dass Mitarbeiter des ärztlichen Dienstes nach Ausscheiden aus der Psychiatrischen Klinik weiterhin Schlüssel der Klinik behielten. Dadurch und durch die Verwendung von Gruppenschlüsseln war es ehemaligen Bediensteten unerlaubterweise möglich, weiterhin auf Patientenakten zuzugreifen, die sich in den Ärztezimmern befanden.

Diese schwer wiegende Verletzung der Zugangs- und Zugriffssicherheit habe ich beanstandet und die Psychiatrische Klinik aufgefordert, entsprechende technische und organisatorischer Maßnahmen (revisionsfähige Schlüsselverwaltung, zugriffssichere Aufbewahrung von Akten, Einbindung des internen Datenschutzbeauftragten des Klinikums bei der Definition und Umsetzung entsprechender Sicherheitsmaßnahmen) zur Vermeidung einer Wiederholung eines vergleichbaren Vorgangs zu ergreifen.

Aufgrund meiner Beanstandung wurde von Seiten der Klinikleitung sofort eine Dienstanweisung erlassen, die grundlegende Verhaltensnormen im Umgang mit Patientendaten und Schlüsseln der Klinik zum Inhalt hat. Weiterhin wurden in den Bereichen des Klinikums, in dem sensible Akten gelagert sind und bei den Oberarztzimmern neue Schließzylinder eingebaut, die einem sehr be-

grenzten Berechtigungsmodus unterliegen. Darüber hinaus erhielt jedes Arztzimmer ein neues Schrankschließsystem zur Aufbewahrung von Akten, dessen Schlüssel nicht mehr mit dem jeweiligen Türschloss übereinstimmt.

Im Rahmen der finanziellen Möglichkeiten soll für die sensiblen Bereiche der Klinik eine Zugangskontrolle durch ein Electronic Key-System sichergestellt werden. So wurden bereits 10 Türen der Klinik mit derartigen elektronischen Schlössern ausgerüstet, die nunmehr ohne Besitz eines entsprechend codierten Schlüssels von außen nicht mehr geöffnet werden können.

Die Vorfälle in der Psychiatrischen Klinik wurden vom internen Datenschutzbeauftragten zum Anlass genommen, auch die anderen Kliniken des Kopfklinikums zu begehen und entsprechende Vorschläge zur Sicherstellung des Datenschutzes in diesen Bereichen zu unterbreiten.

Patientendaten im Internet

Ein Institut eines anderen Klinikums hatte auf seiner Website Laborberichte über Patienten so ungenügend anonymisiert, dass durch die teilweise immer noch erkennbaren Namen, die Geburtsdaten und in Einzelfällen die einliefernde Station die betreffenden Personen zumindest für deren näheren Bekanntenkreis erkennbar waren. Dazu waren die Namen ungekürzt über den Quellcode der Dokumente und über das Dateiverzeichnis zugänglich. Die Laborberichte enthielten neben den genannten Hinweisen auf die jeweilige Person eingehende Daten über die Laborbefunde der Patienten.

Durch diesen Vorgang wurde nicht nur gegen das Bayerische Datenschutzgesetz sondern auch gegen das Bayerische Krankenhausgesetz verstoßen. Danach sind für Patientendaten besondere Schutzmaßnahmen zu treffen, so dass diese Informationen nicht unbefugten Dritten bekannt werden. Durch den unsachgemäßen Umgang mit den Datenverarbeitungstechniken standen im Gegensatz dazu die medizinischen Werte mehrerer hundert Personen dem Zugriff von Nichtberechtigten, nämlich der Internetgemeinde auf der ganzen Welt, offen.

Neben der förmlichen Beanstandung wurde dem Klinikum ein Katalog von Maßnahmen an die Hand gegeben, damit derartige grobe Mängel in Zukunft verhindert werden. Unter anderem wurde das Klinikum aufgefordert, die Web-Seiten anderer Institute auf etwaige unbefugte Veröf-

fentlichung von personenbezogenen Daten zu überprüfen und es wurden Hinweise zur Gestaltung von Web-Seiten gegeben, damit nicht nochmals aufgrund einer unsachgemäßen Gestaltung unbeabsichtigt Zugriff auf vertrauliche Informationen eröffnet wird.

Ich habe den Vorfall weiter zum Anlass für allgemeine Hinweise an Behörden und andere öffentliche Stellen zur datenschutzgerechten Informationsgestaltung in Internet und Intranet genommen. Diese Hinweise klären über zulässige Inhalte in Behörden-Websites auf und enthalten technische und organisatorische Ratschläge für eine sichere und datenschutzgerechte Veröffentlichung von Informationen auf Web-Servern. Diese Orientierungshilfe zur „Veröffentlichung von Informationen im Internet und im Intranet“ ist auf meiner Homepage (www.datenschutz-bayern.de/inhalte/technik.htm) abrufbar.

17.2.2 Erkenntnisse aus Prüfungen

Neben den beiden beanstandeten Kliniken und einigen Nachprüfungen habe ich folgende Dienststellen nach Art. 7 BayDSG (teilweise in Verbindung mit § 9 BDSG und Anlage) im Berichtszeitraum unter technisch-organisatorischen Aspekten kontrolliert:

- AOK-Direktion Hof
- AOK-Dienstleistungszentrum Ärzte in Nürnberg
- AOK-Pflegekasse in Kulmbach
- Bayerisches Rotes Kreuz (Netzwerk des Präsidiums, Bergwachtabschnitt Allgäu)
- Bezirkskrankenhaus Gabersee
- IKK Oberbayern
- Kassenzahnärztliche Vereinigung Bayerns
- Kliniken der Friedrich-Alexander-Universität in Erlangen (Rechenzentrum)
- Klinikum Innenstadt der Ludwig-Maximilians-Universität München (Abteilung für Infektions- und Tropenmedizin)
- Kreiskrankenhäuser Cham, Kötzting und Roding
- Landwirtschaftliche Sozialversicherungsträger Unterfranken
- Landeshauptstadt München (Gesundheitshaus)
- Landratsamt Kulmbach

- Stadt Erlangen
- Stadt Immenstadt im Allgäu
- Stadt Rehau
- Universität Bamberg
- Universität Bayreuth
- Universität Würzburg (Klinikverwaltung)
- Vertrauensstelle des Bayerischen Krebsregisters

Ergebnisse der Kontrolltätigkeit

Ich konnte wiederum einigen Dienststellen bescheinigen, dass die Datensicherheit nahezu vorbildlich gewährleistet ist. Allerdings fand ich auch in diesem Berichtszeitraum wieder einige schwer wiegendere Mängel vor, auf die ich nachfolgend etwas ausführlicher eingehen möchte:

Verschlüsselung

Wie ich unter Nr. 17.1.2 eingehend ausgeführt habe, ist beim Versand von Nachrichten und sonstigen Informationen über das Internet zu berücksichtigen, dass das Internet ein offenes Netz ist und von sich aus derzeit keinerlei Schutzmechanismen zur Wahrung der Vertraulichkeit, Integrität und Authentizität bietet. Deshalb sind alle über das Internet zu versendenden schutzwürdigen Daten (z. B. bei Versand per E-Mail oder mit FTP) zu verschlüsseln und soweit möglich digital zu signieren. Dies setzt voraus, dass der Empfänger auch über entsprechende Vorrichtungen verfügt, die es ihm gestatten, die Zeichenfolge wieder zu entschlüsseln und die Signatur zu verifizieren.

Wichtig ist dabei, dass bei E-Mails nicht nur die Nachrichten selbst verschlüsselt werden, sondern auch deren Anlagen, soweit schutzwürdige Inhalte gegeben sind. Dies wird leider vielfach nicht beachtet.

Als hinreichend sichere Algorithmen gelten derzeit beispielsweise Triple-DES mit 112 oder IDEA mit 128 Bit Schlüssellänge. Für asymmetrische Verfahren wie RSA wird empfohlen, eine Schlüssellänge von wenigstens 1024 Bit zu verwenden. Softwareprodukte dazu stehen im Internet sowie auf dem Markt zur Verfügung.

Eine Verschlüsselung der internen E-Mails ist immer dann durchzuführen, wenn personenbezogene Daten übertragen werden, die anderen Mitarbeitern (also auch den Systemverwaltern) nicht zur Kenntnis gelangen dürfen und der unerlaubte Zugriff auf die E-Mails nicht ausgeschlossen werden kann.

Einsatz von „diskless"-PC und Sperrung der Schnittstellen

Im PC-Netz sollten nur so genannte „diskless"-PC eingesetzt werden. Vorhandene Disketten- und CD-ROM-Laufwerke sollten entweder ausgebaut oder wie nicht benötigte Schnittstellen im BIOS gesperrt werden.

Der Zugriff auf das BIOS sollte zur Verhinderung unerlaubter Systemeinstellungen mit einem Kennwortschutz versehen werden.

EDV-Personal

Manche Dienststellen verfügen nicht über das zur Erfüllung der Aufgaben erforderliche EDV-Personal. Dies stellt ein großes Risiko für die Gewährleistung der Ausfallsicherheit und der Ordnungsmäßigkeit der Datenverarbeitung dar. So ist beispielsweise häufig die Vertretung des Systemverwalters nicht geregelt.

Wegen der raschen Fortentwicklung der IT-Technik ist das Fachpersonal regelmäßig und ausreichend zu schulen. Anbieter von Softwarepaketen in kommunalen Bereich bieten beispielsweise ihren Kunden an, deren EDV-Personal entsprechend auszubilden (z. B. zu NT-Administratoren).

Faxversand

Auch bei einem Versand von personenbezogenen Daten per Fax müssen Maßnahmen getroffen werden, die verhindern, dass bei der Übertragung diese Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Somit müssen beim Versand personenbezogener Daten mittels **Telefaxgerät** entsprechende Zusatzmaßnahmen ergriffen werden. So sollte beispielsweise der zu übertragende Text zur Sicherheit gegen Lauscher auf dem Übertragungsweg durch geeignete Verfahren verschlüsselt werden. Dies setzt natürlich voraus, dass der Empfänger über entsprechende Vorrichtungen verfügt, die es ihm gestatten, den Text wieder zu entschlüsseln.

Da derartige Vorrichtungen bei einem **Fax-Versand mittels PC** aufgrund des verwendeten Protokolls derzeit noch nicht zur Verfügung stehen, muss – außer wenn dadurch in einem Notfall eine nicht zumutbare Zeitverzögerung entstehen würde – ein Versand sensibler personenbezogener Daten online per Fax unterbleiben.

Als weitere Möglichkeit zur Gewährleistung der Sicherheit bei der Datenübertragung könnten identifizierende personenbezogene Merkmale durch ein Pseudonym ersetzt und die Zusammenführung von Pseudonymen und personenbezogene Daten auf einem getrennten Weg (z. B. mittels Telefon) durchgeführt werden. Dies stellt allerdings einen erheblichen organisatorischen Aufwand dar.

Auf jedem Fall sind die üblichen Sicherheitsmaßnahmen zu beachten wie Sicherstellung der Empfängernummer, Sicherstellung, dass nur der berechtigte Empfänger das Fax erhält.

E-Mail

Wendet sich ein Betroffener per E-Mail an eine Behörde, so hat die Behörde bei ihrer Antwort zu prüfen, ob der Inhalt schutzwürdige Daten enthält. Ist das der Fall, muss diese E-Mail verschlüsselt versandt werden. Wenn der Absender seinen Schlüssel nicht angegeben hat, muss die Behörde diesen entweder erfragen oder die Antwort auf herkömmliche Art mit der Post in einem verschlossenen Umschlag versenden. Es darf keinesfalls der Schluss gezogen werden, wenn der Anfragende eine unverschlüsselte E-Mail schickt, kann die Behörde diesen Versandweg ebenfalls ungeprüft nutzen.

17.2.3 Erkenntnisse aus Beratungen

Zusätzlich habe ich wieder zahlreiche Dienststellen hinsichtlich der Datensicherheit beraten, wobei im zunehmenden Maße die Gefahren bei einem Öffnung der lokalen Netze nach außen (insbesondere bei einem **Internetanschluss**) und die dabei zu ergreifenden Sicherheitsmaßnahmen Gegenstand der Beratungen waren. Insbesondere sollte für die Internetbenutzung eine entsprechende Richtlinie erarbeitet werden, die allen Nutzern gegen Unterschrift auszuhändigen ist. Eine entsprechendes Muster (Grundsätze für „Benutzerrichtlinien für den Umgang mit Internet“) ist auf meiner Homepage (www.datenschutz-bayern.de/inhalte/technik.htm) abrufbar.

Auch bei der Entwicklung geeigneter Sicherheitskonzepte für **Intranets** (insbesondere Landkreis-Behördennetze) wird meine Geschäftsstelle immer häufiger beteiligt. Ich habe dies zum Anlass genommen, eine Orientierungshilfe „Datensicherheit beim Betrieb eines Landkreis-Behördennetzes (Intranet)“ - Kommunales-Behördennetz - zu erstellen. Auch diese Orientierungshilfe ist auf meiner Homepage unter www.datenschutz-bayern.de/inhalte/technik.htm abrufbar.

Viele Behörden sind auch aufgrund der immer häufiger werdenden **Virenwarnungen** verunsichert. Während es bis vor einiger Zeit war noch ausreichend war, Arbeitsplatzrechner ohne Disketten- und ohne CD-ROM-Laufwerk auszustatten, um den Import von Viren abzuwehren, wurde durch den Anschluss an öffentliche Netze (insbesondere an das Internet) eine weit größere Gefahr für die Verbreitung von Viren geschaffen. So können Viren durch den E-Mail-Verkehr, beim Websurfen oder durch das Herunterladen von Dateien eingeschleust werden. Näheres zu diesen neuen Virenarten und Möglichkeiten ihrer Bekämpfung ist im vorhergehenden Punkt „Viren im Internet“ zu finden und kann außerdem meiner oben genannten Orientierungshilfe „Datensicherheit beim Betrieb eines Landkreis-Behördennetzes (Intranet)“ - Kommunales Behördennetz - (abrufbar unter www.datenschutz-bayern.de/inhalte/technik.htm) entnommen werden.

17.3 Technische Einzelprobleme

17.3.1 Prüfungsverwaltungssystem FlexNow!

Mitte 1999 besuchte einer meiner Mitarbeiter die Otto-Friedrich-Universität Bamberg, um sich über den Stand der technischen und organisatorischen Datenschutz- und Datensicherheitsmaßnahmen u.a. im Verfahren FlexNow! zu unterrichten. Das Verfahren FlexNow! ist Teil eines Modellversuches für ein „Flexibles Studien- und Prüfungssystem“ in der Fakultät Sozial- und Wirtschaftswissenschaften der Otto-Friedrich-Universität Bamberg und wird seit 1994 am Lehrstuhl Wirtschaftsinformatik entwickelt. FlexNow! befindet sich derzeit im Übergangsstadium vom Projekt zur Produktivanwendung für die Universitätsverwaltung.

Im fachlichen Kern von FlexNow! werden die Prüfungs- und Studienordnungen abgebildet. Es ist ein Anwendungssystem zur Verwaltung von studentischen Prüfungsdaten, das vom Studenten auch über das Internet genutzt werden kann. FlexNow! unterstützt den gesamten Prüfungsprozess von der Erstellung des Prüfungsangebotes über die Prüfungsanmeldung, die Prüfungslogistik, die Erfassung der Prüfungsergebnisse bis hin zur Erstellung von Bescheiden und Zeugnissen.

FlexNow! ist als Client-Server-System ausgebildet. Die möglichen FlexNow!-Clients sind in zwei Kategorien unterteilbar, nämlich in spezifische Client-Anwendungen für die vier Nutzergruppen Prüfungsamt, Prüfungsausschuss, Lehrstuhl und Verwaltung mit rollenbasierter und z.T. zeitlich begrenzter Zugriffsmöglichkeit auf den FlexNow!-Datenbank-Server sowie in WWW-Browser-Anwendungen der Studierenden für den Zugriff auf den FlexNow!-WWW-Server.

Die WWW-Browser der Studierenden greifen über das Internet auf den WWW-Server von FlexNow! zu, der vom FlexNow!-Datenbank-Server mit Daten gespeist wird. So kann von den Studierenden das Prüfungsangebot abgerufen, die An- und Abmeldung zu bzw. von Prüfungen innerhalb der Meldefristen durchgeführt und ein persönlicher Prüfungsplan für das Semester erstellt werden. Außerdem kann der Studierende jederzeit und von jedem Ort aus seinen vollständigen Datensatz u.a. mit Studienhistorie und aktuellen Prüfungsergebnissen abrufen. Für Identifizierung und Authentifizierung gelangt die aus dem Bereich des Home-Bankings bekannte Methodik des PIN-TAN-Verfahrens zur Anwendung. Um einen höheren Grad an Sicherheit bei

der Authentifizierung und Datenübertragung über das Internet zu erreichen, ist beabsichtigt, spezifische Produkte (TranSON) und Protokolle (SSL) zu verwenden.
Zur Steigerung des Datensicherheits- und Datenschutzniveaus habe ich eine Reihe von Forderungen erhoben und auch Empfehlungen ausgesprochen, wie z.B. Erteilung der datenschutzrechtlichen Freigabe nach Art. 26 BayDSG, physikalische Trennung des Datenbankservers vom WWW-Server, zügige Einführung von kryptografischen Maßnahmen zur Sicherung der Datenübertragungen über das Internet, Begrenzung der Gültigkeitsdauern der Passworte und systemseitige Erzwingung eines Passwortwechsels nach ca. 90 Tagen, verschlüsselte Speicherung der Passworte, Verwendung von persönlichen Benutzerkennungen und Passworten anstatt der gemeinsamen Nutzung der gleichen Benutzerkennung und des gleichen Passwortes durch mehrere Lehrstuhlmitarbeiter, Begrenzung der Anzahl an unmittelbar aufeinander folgenden Anmeldeversuchen mit entsprechenden Systemreaktionen sowie Festlegung der Aufbewahrungsdauer von Protokollierungsdaten.

Meine Anregungen wurden sehr offen aufgenommen, aber noch nicht vollständig umgesetzt. Es ist auch festzustellen, dass bereits bei der Konzeption des Verfahrens den Aspekten der Datensicherheit und des Datenschutzes ein hoher Stellenwert beigemessen wurde. So hat der Lehrstuhl für Wirtschaftsinformatik der Otto-Friedrich-Universität Bamberg auch eine umfangreiche Ausarbeitung zu Datenschutz und Datensicherheit mit Sicherheitsrichtlinien und Empfehlungen erstellt, um so auch für die Fälle einer Verwendung von FlexNow! an anderen Universitäten eine konstruktive Hilfestellung bzgl. dieser Aspekte zu geben.

Trotz dieser erfreulichen Umstände wäre es m.E. hilfreich gewesen, wenn ich zu einem noch früheren Projektstadium eingebunden worden wäre.

FlexNow! wird auch bereits an weiteren Universitäten in Deutschland (Saarbrücken, Göttingen, Augsburg, Münster) und Österreich (Graz) eingesetzt. Weitere Installationen werden vorbereitet, befinden sich in Einführung oder sind projektiert (z.B. München, Hamburg, Gießen, Marburg, Regensburg, Erfurt, Bayreuth, Bremen). Die Verwaltungskomponente der Virtuellen Hochschule Bayern wurde auf der Basis von FlexNow! realisiert.

17.3.2 Projekt RegioSignCard

Im Rahmen des bundesweiten Städtewettbewerbs MEDIA@Komm wurde auch der von der Nürnberger Initiative für die Kommunikationswirtschaft e.V. NIK e.V. im Namen des Städteverbundes Nürnberg-Fürth-Erlangen-Schwabach-Bayreuth eingereichte Projektantrag „RegioSignCard“ prämiert; er wird nunmehr aus Bundesmitteln gefördert. In der NIK sind neben diversen privatwirtschaftlichen Unternehmen auch die genannten Städte vertreten. Ziel dieses Projekts ist die Errichtung virtueller Dienstleistungszentren (virtuelles Rathaus und virtueller Marktplatz) und vor allem der Aufbau einer sicheren und Rechtsverbindlichkeit erlaubenden Kommunikationsinfrastruktur, die von Institutionen, Firmen und vor allem von Bürgern genutzt werden soll. Träger für die Umsetzung dieses Projekts ist die Curiavant Internet GmbH, eine von den fünf Städten gegründete Firma (der ursprüngliche Name Makon GmbH musste wegen der Nichtverfügbarkeit der Domäne makon.xxx geändert werden).

Das Projekt definiert für die Zielgruppen

- Kommunen und Kammern als Anbieter öffentlicher Dienste für Bürger und Unternehmen,
- Rechtsfähige Bürger als Nutzer der öffentlichen Dienste und der Angebote privatwirtschaftlicher Unternehmen,
- Privatwirtschaftliche Unternehmen als Nutzer öffentlicher Dienste und als Anbieter eigener Dienste für ihre Kunden

als Hauptnutzen die „Einführung der Digitalen Signatur und Sicherstellung einer vertraulichen Kommunikation“.

Als eines der Hauptprobleme technischer Art zur Realisierung dieser grundlegenden Datensicherheitsanforderung gilt, wie aus allen ähnlichen Projekten bekannt, das bei allen Beteiligten unterschiedliche Spektrum von Hard- und Softwarekomponenten. Das hat zur Folge, dass Komponenten und Mechanismen definiert und gefunden werden müssen, die auf allen gängigen Plattformen zum Ablauf kommen können. Somit ist auch die Schaffung einer kompatiblen Anwendungsumgebung ein erklärtes Ziel dieses Projektes. Die Kompatibilität aller am Markt gebräuchlichen Hard- und Softwaresysteme zur Erzeugung und Verifizierung der Digitalen Signatur sollte ebenso gewährleistet sein, wie der Einsatz von Chipkarten, die von unterschiedlichen

Trust Centern ausgegeben werden. Außerdem müssen auch die Verschlüsselungsverfahren untereinander verträglich sein.

Die Akzeptanz eines solchen Systems hängt von der Attraktivität der Anwendungen, der Benutzerfreundlichkeit und natürlich auch von der Sicherheit ab. Ein virtueller Marktplatz lebt von der Vielfalt der Angebote und Anbieter, das virtuelle Rathaus von der Vielfalt der Angebote. Alle Anbieter haben gewisse Investitionen zu tätigen, die sich wiederum dann schneller amortisieren, wenn sie möglichst viele Benutzer in Anspruch nehmen. Benutzerfreundlichkeit setzt aber nicht nur eine einfache Bedienung voraus, sondern hat selbstverständlich auch eine Kostenkomponente. Das heißt, der Anwender muss sowohl für das Equipment als auch für die genutzten Dienste bezahlen.

In diesem Projekt soll die Prozessor-Chipkarte mit Digitaler Signatur, Geldkarte und Platz für Zusatzanwendungen (z.B. Betriebsausweis, Fahrscheine für den öffentlichen Nahverkehr) sowohl zur rechtsverbindlichen Unterschrift, zur Abwicklung von Banktransaktionen, zur Identifizierung und auch zur Verschlüsselung verwendet werden. Um Kosten zu sparen, bietet sich diese Kombinationskarte an, die als Bankkarte, als Signaturkarte, als Geldkarte und als Zugangsinstrument in den verschiedensten Anwendungen (z.B. als Betriebsausweis) genutzt werden kann. Die Personalisierung solcher Kombinationskarten leisten Trust Center, die den Anforderungen des Signaturgesetzes entsprechen (z.B. die Telesec, die Post und später auch Banken). Um die Chipkarte einsetzen zu können, benötigt der Benutzer dann noch einen Kartenleser und Kommunikations- und Verschlüsselungssoftware an seinem PC.

Die Kommunikationsplattform wurde beispielhaft auf der Grundlage des BROKAT-Twister konzipiert, der sich im Bankbereich bewährt hat und die Anforderungen einer integrierten Lösung erfüllt. Eine solche Plattform muss die verschiedenen Dienste zur Verfügung stellen, die für Abwicklung und Sicherheit notwendig sind und zusätzlich die Welt des Internet mit den PC-Systemen mit der Welt der Hostrechner verbinden, auf denen in den meisten Firmen und Verwaltungen die Anwendungen laufen und die relevanten Daten gespeichert sind. Hierzu muss die heterogene Hard- und Software der Partnerstädte und der beteiligten Firmen und Institutionen beherrschbar integriert werden. Das Sicherheitskonzept baut auf der digitalen Signatur oder allgemeiner auf der Nutzung von zuverlässig erzeugten, verteilten und gespeicherten Zertifikaten

auf; diese werden außer zur Signaturerzeugung auch als Authentifizierungs- und Identifikationsinstrument genutzt. Mit Hilfe der Verschlüsselung auf der Basis von SSL wird bei der Kommunikation ein hohes und ausreichendes Maß an Vertraulichkeit erreicht. Diese zwischen Client und Server der jeweiligen Firma, Institution oder Verwaltung im Hintergrund immer aktive Verschlüsselung soll zur Erhöhung der Sicherheit bei Übertragung und Speicherung durch eine zusätzliche Ende-zu-Ende-Verschlüsselung bzw. Archivverschlüsselung ergänzt werden. Selbstverständlich müssen alle Anwendungen gegeneinander abgeschottet werden. Ein privatwirtschaftliches Unternehmen darf genauso wenig Zugriff zu Verwaltungsdaten haben, wie eine Behörde zu den Daten eines Wirtschaftsunternehmens.

Chipkarten (z.B. die E4/hoch evaluierten und damit SigG-konformen Karten der Telesec und der Post), Signaturmechanismus (RSA 1024 Bit), Verschlüsselungsverfahren (z.B. IDEA 128 Bit, SSL 128 Bit) und entsprechend ausgerichtete und dem SigG entsprechende Hard- und Software (verschiedene Anbieter) stehen am Markt zur Verfügung, so dass aus der Sicht der Datensicherheit nicht der bei ähnlichen Projekten manchmal festzustellende Nachholbedarf besteht. Die ersten Prototypen eines Bürgerterminals wurden im 2. Halbjahr 2000 im Rahmen des Projektes Media@Komm im genannten Städteverbund für die Anwendungen „Beantragung eines Anwohnerparkausweises“ und „Mülltonnenbestellung“ bereitgestellt und werden im tatsächlichen Betrieb getestet. Feldversuche mit anschließendem Wirkbetrieb sind in größerem Umfang in 2001 zu erwarten, wenn die Multifunktionskarte mit den beschriebenen Funktionen von den Banken herausgegeben und damit das Instrument Chipkarte mit Digitaler Signatur, Geldkarte und Zusatzfunktionen in hohen Stückzahlen verbreitet wird.

Das Verfahrenskonzept lässt keine Sicherheitsdefizite erkennen.

17.3.3 Wartung medizin-technischer Anlagen

In Krankenhäusern und Arztpraxen werden heute moderne medizin-technische Anlagen eingesetzt, die neben Bildern von Körperteilen oder Organen bestimmter Patienten auch identifizierende Patientendaten speichern. Dass diese Geräte regelmäßig gewartet werden müssen, steht außer Zweifel. Grund für eine Wartung ist meist die Sicherstellung der Bildqualität.

Laut Angaben eines renommierten Herstellers von medizin-technischen Geräten soll beim so genannten Remote Service lediglich in 1 Prozent aller Wartungsfälle ein Zugriff auf identifizierende Patientendaten erforderlich sein. Erfolgt beim Remote Service kein Zugriff auf identifizierende Patientendaten kann auf spezielle Sicherungsmaßnahmen verzichtet werden.

Bei 99 Prozent aller Wartungsfälle ist demnach ein Zugriff auf Patientendaten nicht notwendig, das heißt, die Patienten identifizierenden Merkmale können entweder generell ausgeblendet oder vor Beginn der Wartungsarbeiten durch Pseudonyme ersetzt werden.
Ist im Rahmen der Gerätewartung der Zugriff auf identifizierende Patientendaten unvermeidlich, sind folgende Maßnahmen einzuhalten:

- Einsatz eines Call-Back-Verfahrens oder eines ähnlichen Verfahrens (Dialogaufbau vom Kundensystem oder nach Ablauf einer so genannten Shake-Hand-Prozedur).
- Verwendung eines sicheren Passwortverfahrens (u.U. Verwendung von Einmalpassworten).
- Protokollierung des gesamten Fernwartungsdialogs, aus dem alle Aktionen und Zugriffe auf Patientendaten erkennbar sind.
- Der Dialog sollte von einem sachkundigen Mitarbeiter des Krankenhauses oder in der Arztpraxis verfolgt werden.
- Bei der Übertragung der Daten muss ihre Vertraulichkeit sicher gestellt werden können (Einsatz von geeigneten Verschlüsselungsverfahren).
- Benutzung des Internets nur, wenn Anwendungs- und Herstellersystem durch geeignete Firewall-Systeme vom offenen Netz abgeschottet sind.
- Soweit erforderlich, dürfen personenbezogenen Patientendaten in der Fernwartungszentrale nur temporär gespeichert werden.
- Einsatz von zuverlässigem Personal bei der Wartungsfirma (Verpflichtung auf Geheimhaltung).
- Schriftlicher Vertrag mit der Wartungsfirma (Einhaltung des Datengeheimnisses und der gebotenen Sicherheitsmaßnahmen; Schadenersatzklausel).

Die beste Lösung wäre es allerdings, wenn es möglich wäre, bei der Wartung lediglich auf eine signifikante Testumgebung zuzugreifen, so dass der Zugriff auf identifizierende Patientendaten vermieden würde. Auch das Ersetzen der identifizierenden Merkmale durch ein Pseudonym stellt eine datenschutzfreundliche Alternative dar.

17.3.4 Sicherheit in medizinischen Netzen

Der elektronische Austausch medizinischer Daten insbesondere die Anwendungen der Telemedizin schreitet stetig voran. Viele Anbieter von medizinischen Netzen sehen mittlerweile ausreichende Maßnahmen zur Datensicherheit vor. Wegen der Bedeutung dieses Themas für den Datenschutz und die Datensicherheit wurden die Forderungen aus dem letzten Tätigkeitsbericht an die Entwicklungen angepasst.

Bei der Übertragung von Patientendaten aller Art (Arztbriefe, Untersuchungsergebnisse, E-Mails, Bilder) in offenen Netzen, wozu letztlich auch das Bayer. Behördennetz oder die Landkreisnetze zählen, sind geeignete Sicherheitsmaßnahmen zu ergreifen, damit die Vertraulichkeit und Integrität der übertragenen Daten sowie die Revisionsfähigkeit der Netzbenutzung und den Zugriffsschutz der angeschlossenen DV-Systeme sichergestellt sind.

- Das DV-System darf nur solchen Benutzern Zugang zum Netz erlauben, die sich sowohl als Berechtigte identifizieren können, als auch vom DV-System als Berechtigte erkannt werden (Authentisierung). Die berechtigten Benutzer können auch unterschiedliche Rechte besitzen. Als Träger für die Autorisierungsdaten bietet sich die Chipkarte an. Die Rechner, die die Verbindung zum Netz herstellen, und vor allem die internen Netze sind durch geeignete Sicherheitsmaßnahmen, wie z. B. Schutz durch ein Firewall-System gegen unberechtigte und ungewollte Eindringversuche von außen (Veränderung von Software, Manipulation von Daten, Ausspähen von Informationen), abzusichern.

- Die Integrität der im Netz übertragenen Patientendaten lässt sich durch die heute bereits verfügbaren Signaturverfahren verifizieren. Durch die digitale Signatur lassen sich Dokumente außerdem eindeutig zuordnen. Der Empfänger eines Dokuments kann an der digitalen Signatur den Autor des Dokuments erkennen. Auch dazu haben sich die Chipkarten als Träger der Signaturschlüssel und der Signaturverfahren bewährt.

- Die Vertraulichkeit aller auf dem Netz übertragenen Patientendaten kann nur durch geeignete Verschlüsselungstechniken gewährleistet werden. Dabei ist insbesondere zu beachten, dass die zum Einsatz kommenden Verfahren gegen Entschlüsselungsversuche hinreichend sicher sind. Auf meine Ausführungen im 18. Tätigkeitsbericht (Tz. 19.1.4) wird verwiesen.

- Jedes an der Kommunikation mit Patientendaten beteiligte DV-System muss für jeden bestimmten Einzelfall zur Beweissicherung Empfangs- und Übergabenachweise aufzeichnen,

damit dokumentiert ist, wer wann an wen welche Patientendaten übertragen oder empfangen hat (Protokollierung).

- Werden Patientendaten außerhalb eines Klinikums, Krankenhauses oder einer Arztpraxis zwischengespeichert, müssen sie verschlüsselt sein. Die Schlüssel müssen gegenüber dem Netzbetreiber geheim gehalten werden, sie dürfen nur im Besitz des medizinischen Personals sein.

Diese Forderungen gelten auch in der Telemedizin für die Übertragung von Röntgenbildern oder sonstigen medizinischen Bildern (Computer-Tomographie, Ultraschall o.ä.), sofern diese Angaben enthalten, die einen bestimmten Patienten identifizieren. Da die Verschlüsselung von Bildern noch mehr von Bewegtbildern recht zeitaufwendig werden kann, sollte man hier Pseudonyme verwenden, die Außenstehenden keine Zuordnung zu einer bestimmten Person erlauben.

17.3.5 Backup-Service

Viele, insbesondere Anwender von Standardsoftware fahren zwar ihre täglichen Sicherungen, prüfen jedoch nicht, ob diese Sicherungen vollständig und korrekt sind. Hinzu kommt, dass vielfach beim Anwender gar nicht das Know-how vorhanden ist, nach einem Systemzusammenbruch mit den Sicherungsbeständen einen Wiederanlauf erfolgreich durchzuführen.

So gibt es heute Anbieter, die die Sicherungsbestände unter Anwenderbedingungen auf ihre Verwendbarkeit hin testen. Eine solche Dienstleistung ist für viele Anwender wertvoll und unverzichtbar, wenn man bedenkt, dass wegen fehlerhafter Datensicherungen Datenverluste auftreten können. Das kann im ungünstigsten Fall sogar dazu führen, dass die Datenbestände unter Umständen überhaupt nicht mehr rekonstruierbar sind. Aus diesem Grunde sollten zumindest die halb- oder vierteljährlich gezogene Datensicherungen auf ihre Verwendbarkeit hin überprüft und als Katastrophensicherungen bis zur nächsten getesteten Vollsicherung unbedingt aufbewahrt werden.

Einige Hersteller von Standardanwendungssystemen bieten ihren Kunden einen so genannten Backup-Service an. Gerade kleinere Anwender, insbesondere aus dem Kommunal- und Gesund-

heitsbereich, sind häufig nicht dazu in der Lage, qualifizierte DV-Mitarbeiter zu beschäftigen. Da diese Anwender heute aber in einem immer größer werdenden Maße von der Verfügbarkeit ihrer DV-Anwendungen abhängig sind, sollten sie diesen Service nutzen, ihre tägliche gezogene Datensicherung bei Experten auf ihre Brauchbarkeit hin untersuchen zu lassen. Auf diese Weise kann frühzeitig – also bereits vor dem Eintritt eines K-Falls – auf Fehler und Unstimmigkeiten in der Datensicherung reagiert werden.

17.3.6 Verarbeiten von Daten des Gesundheitsamtes im Landratsamt

Eine Reihe von Staatlichen Gesundheitsämtern, die durch die Behördenverlagerung eine Abteilung des Landratsamtes geworden sind, hat im Berichtszeitraum die Frage an mich herangetragen, ob und unter welchen Voraussetzungen Daten des Staatlichen Gesundheitsamtes (Gesundheitsabteilung) auf den Rechnern des Landratsamtes verarbeitet werden können.

Beim Anschluss des Gesundheitsamts an die DV-Anlage des Landratsamts stellt sich zunächst rechtlich die Frage, ob der für das Gesundheitsamt tätige Amtsarzt durch die Mitwirkung des DV-Spezialisten des Landratsamts bei der Verarbeitung der vom Arzt erhobenen Daten Verschwiegenheitspflichten (§ 203 StGB, Art. 6 GDG) verletzt. Eine Straftat im Sinne von § 203 Abs. 1 Nr. 1 StGB liegt nur dann vor, wenn der Arzt die Daten „unbefugt“ offenbart. Das ist hier aber nach der in der Literatur vertretenen Auffassung dann nicht der Fall (Rechtsprechung dazu gibt es allerdings bisher nicht), wenn der DV-Spezialist als „berufsmäßig tätiger Gehilfe“ i. S. von § 203 Abs. 3 StGB angesehen werden kann.

Dazu ist es notwendig, dass der DV-Mitarbeiter insoweit alleine dem Gesundheitsamt unterstellt und hier den alleinigen Weisungen des Amtsarztes unterworfen ist. Für deren Hinzuziehung im Rahmen des Erforderlichen kann das konkludente Einverständnis des Betroffenen angenommen werden, da jeder Arzt oder sonstige Geheimnisträger i. S. von § 203 Abs. 1 StGB bei seiner Tätigkeit darauf angewiesen ist, von „berufsmäßig tätigen Gehilfen“ unterstützt zu werden und diese „Gehilfen“ daher gemäß § 203 Abs. 3 StGB den Geheimnisträgern gleichgestellt und ebenfalls zur Verschwiegenheit verpflichtet sind. Zu den berufsmäßig tätigen Gehilfen i. S. von § 203 Abs. 3 StGB zählt auch internes technisches Fachpersonal, da es den Geheimnisträger bei seinen Aufgaben unterstützt. Durch seine Einbeziehung in § 203 Abs. 3 StGB in den Kreis der Schwei-

gepflichtigen wird das Patientengeheimnis hinreichend geschützt. Der DV-Spezialist des Landratsamts sollte auf seine besondere Verschwiegenheitspflicht nach § 203 Abs. 1 und 3 StGB schriftlich hingewiesen werden. Ich muss allerdings darauf hinweisen, dass die Frage, ob eine Schweigepflichtverletzung vorliegt, verbindlich nur im Einzelfall von den Staatsanwaltschaften und zuständigen Gerichten beantwortet werden kann. Meine oben getroffene Auskunft ergibt sich aus der Sicht des Datenschutzes.

Bei einem gemeinsam mit dem Landratsamt betriebenen Rechner ist weiter eine strikte Abschottung der beiden Bereiche unabdingbar. Mitarbeiter des Landratsamtes dürfen keinen Zugriff auf Daten und Verfahren des Gesundheitsamts haben und umgekehrt. Der interne Datenschutzbeauftragte sollte das Zugriffsschutzkonzept vor seinem Einsatz geprüft haben. Die Berechtigungsprofile der einzelnen Mitarbeiter sind außerdem revisionsfähig zu archivieren, damit bei Prüfungen durch die Aufsichtsbehörde auf sie zugegriffen werden kann.

In der Praxis bedeutet das, dass die Schweigepflicht des DV-Personals auch gegenüber dem Landrat gelten muss (§ 203 Abs. 1 Nr. 1 StGB im Sinne Art 6 Abs. 1 Satz 5 GDG). Somit darf das DV-Personal, soweit es Aufgaben des Gesundheitsamts erfüllt und Kenntnis von Daten des Gesundheitsamtes erlangen kann, nur den alleinigen Weisungen des Amtsarztes – nicht aber des Landrats – unterliegen. Wenn das aber im Dienstbetrieb nicht zu gewährleisten ist, gibt es zwei Alternativen:

1. Physikalische Trennung der Datenbestände auf verschiedenen Rechnern

In diesem Falle muss ein eigener File-Server für die Daten des Gesundheitsamtes zur Verfügung gestellt werden, auf den lediglich Bedienstete des Gesundheitsamtes Zugriff haben dürfen. Die Administrierung dieses Rechners darf nur durch Personal des Gesundheitsamtes erfolgen.

2. Verschlüsselte Speicherung der Daten des Gesundheitsamtes auf dem Server des Landratsamtes

Wird aus welchen Gründen auch immer auf die Bereitstellung eines eigenen Servers für das Gesundheitsamt verzichtet, müssen die Daten des Gesundheitsamtes, wenn sie auf dem Server des Landratsamtes gespeichert werden, verschlüsselt werden. Die Entschlüsselung der Daten darf nur Bediensteten des Gesundheitsamtes möglich sein. Zusätzlich sind alle maschinell erzeugten

Protokolle (auf System- und Anwenderebene) insbesondere hinsichtlich des Anlegens der Benutzerberechtigungen für den Zugriff auf die Verfahren des Gesundheitsamtes und der (versuchten) Zugriffe auf diese Daten im Vier-Augen-Prinzip auszuwerten, wobei zumindest eine dieser mit der Auswertung beauftragten Personen nicht dem DV-Personal des Landratsamtes angehören darf. Hierzu böte sich als Kontrollinstanz der behördliche Datenschutzbeauftragte an.

Wie die Ergebnisse bei den Landratsämtern zeigen, scheint der in der Praxis gangbarere Weg, der zu sein, dass für das Gesundheitsamt ein eigener File-Server zur Verfügung gestellt wird, der auch ausschließlich von Bediensteten des Gesundheitsamtes administriert wird.

17.3.7 Druck von Lohnsteuerkarten durch Privatfirmen

Der Anbieter von Softwarepaketen und EDV-Beratung für die Kommunalverwaltung „komuna“ bietet seinen Kunden die Erstellung der Lohnsteuerkarten bei einem Partnerunternehmen (HSH) in Berlin an. Zu diesem Zwecke werden online die zur Erstellung der Lohnsteuerkarten notwendigen Steuerdaten zur HSG Software GmbH in Berlin übertragen. Der Transport der daraufhin erstellten Steuerkarten zu den Gemeinden erfolgt derzeit per UPS.

Während das Bayer. Staatsministerium der Finanzen in früheren ähnlich gelagerten Fällen Bedenken gegen diese Art des Drucks erhob, erachtet es nunmehr die Beauftragung privater Unternehmen für zulässig, wenn die Gemeinden die Wahrung des Steuergeheimnisses sicherstellen, d.h. wenn das eingesetzte Personal des beauftragten Unternehmens nach dem Verpflichtungsgesetz verpflichtet wird und vertraglich geregelt ist, dass ausschließlich diese nach dem Verpflichtungsgesetz verpflichteten Personen tätig werden. Dieser Meinung des Finanzministeriums schließe ich mich an.

Allerdings ist ein Tätigwerden von **Subunternehmen** bzw. nicht beauftragter Unternehmen, deren Personal nicht nach dem Verpflichtungsgesetz verpflichtet wird, durch Aufnahme entsprechender Bedingungen bei der Beauftragung des privaten Unternehmens auszuschließen.

Außerdem wird die Übermittlung von Daten auf elektronischen Daten nur dann für zulässig erklärt, wenn sichergestellt ist, dass ein unberechtigter Datenzugriff nicht erfolgen kann; elektro-

nisch übermittelte Steuerdaten sind nach dem Stand der Technik zu verschlüsseln. Insoweit ist das beauftragte Unternehmen ausdrücklich auf § 30 Abgabenordnung hinzuweisen.

17.3.8 Schutz von Serverräumen

Da die heutigen Server die Rolle der früheren Großrechner weitgehend übernommen haben, insbesondere was die Speicherung und Verarbeitung personenbezogener Daten betrifft, müssen auch ihre Standorte mit Maßnahmen der Zugangskontrolle (Art. 7 Abs. 2 Nr. 1 BayDSG) gegen unbefugten Zutritt und gegen Einwirkungsmöglichkeiten von außen geschützt werden. Dabei sollten sich die vorgesehenen Schutzmaßnahmen an der Sensibilität der auf den Servern gespeicherten Informationen und an den akzeptablen Ausfallzeiten orientieren.

Als Schutzmaßnahmen kommen insbesondere in Betracht:

Festlegung der Zugangsberechtigten
Der Kreis der Zugangsberechtigten zu den Serverräumen ist auf das unbedingt notwendige Personal zu beschränken.

Außen- und Innenhautsicherung
Die Maßnahmen zur Außenhautsicherung sollen sowohl Sicherheitsmaßnahmen gegen Eindringversuche als auch gegen Einwirkversuche beinhalten. Mit Hilfe der Innenhautsicherung soll die Anwesenheit unbefugter Personen in den Serverräumen erkannt werden. So kommen insbesondere folgende Maßnahmen in Frage:

- Tür- und Fensterschutz (einbruch- und durchbruchhemmend, Einsatz einer Einbruchmeldeanlage, Schließkontaktmelder, Glasbruchmelder, Spezialverglasung, Anbringung einer Sicherheitsfolie, automatische Rolladensicherung etc.)
- Installation von Bewegungsmeldern

Zutrittskontrolle
Zur Verhinderung eines unbefugten physischen Zutritts zu den Serverräumen können maschinelle Zutrittskontrollsysteme eingesetzt werden.

Closed-shop-Betrieb
Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, dürfen keinen Zutritt zu den Serverräumen erhalten.

Revisionsfähige Schlüssel- und Chipkartenregelung
Die Schlüssel- und/oder Chipkartenvergabe für die Serverräume muß revisionsfähig erfolgen.

Maßnahmen zur Bekämpfung von physischen Schäden
Insbesondere sind Maßnahmen zum Schutz vor Feuer und Wassereinbrüchen zu ergreifen. Dazu gehört – soweit möglich – auch die Trennung von Servern und Netzverteilern und die Unterbringung in unterschiedlichen Brandabschnitten. Außerdem kommen beispielsweise folgende Maßnahmen in Betracht:

- Vermeidung von wasserführenden Leitungen
- Installation von Feuchtigkeitsmelder
- Einrichtung eines ausreichenden Branddetektionssystems
- Schaffung abgeschlossener Brandabschnitte
- Installation geeigneter Handfeuerlöschgeräte
- Vermeidung unnötiger Brandlasten
- Nutzung von Überspannungsschutzeinrichtungen

17.3.9 TK-LAN-Anbindungen

Im Zuge umfassender Modernisierungmaßnahmen der Sprachkommunikationseinrichtungen werden und wurden in den bayerischen Behörden Telekommunikationsanlagen (TKA) aufgerüstet, ausgetauscht und auch neu beschafft. In den betreffenden, zentral durchgeführten Ausschreibungen waren neben den reinen Telekommunikationsanlagen u.a. auch die Positionen Voice-/Fax- und CTI-Server enthalten.

Um die von o.g. Servern unterstützten Funktionen PC-Fax, E-Mail und CTI (Computer-Telefon-Integration) vom Sachbearbeiter-Arbeitsplatz aus durchführen und nutzen zu können, ist eine Einbindung der TKA oder der von der TKA gesteuerten Server in das lokale Netzwerk (LAN)

notwendig. Sollte die TKA als solche an ein nutzereigenes LAN angebunden sein, könnte über die Fernwartungsfunktion z.B. auf Daten oder Geräte innerhalb des lokalen Netzes bzw. das Behördennetz zugegriffen werden.

Vor Einbindung einer TKA in ein LAN ist also unbedingt zu prüfen, inwieweit zusätzlich Sicherheitsvorkehrungen gegen einen unberechtigten LAN-Zugriff vorzusehen sind. Hierzu kommen z.B. folgende in Betracht:

- Vor Aufnahme der Fernwartungsarbeiten an der TKA werden die TKA-gesteuerten Server von der TKA physikalisch getrennt, da diese Server i.d.R. für Wartungsarbeiten an der TKA auch nicht benötigt werden.

- Sollen an den TKA-gesteuerten Servern Fernwartungsarbeiten durchgeführt werden, so sind diese vor Aufnahme der Fernwartungsarbeiten physikalisch vom LAN zu trennen, wobei ihre Anbindung an die TKA aber bestehen bleibt. Da in diesem Fall ein Zugriff auf die auf diesen Servern gespeicherten Daten möglich ist, sollte diese Alternative nicht gewählt werden, zumal eine Fernwartung dieser Server im Grundsatz nicht erforderlich ist.

- Evtl. sollte auch die Möglichkeit geprüft werden, den Fernwartungszugriff über einen zentralen Einwahlknoten im Behördennetz zu steuern, der die TKA vom LAN trennt und den ISDN-Zugriff durch den TKA-Hersteller von außen freigibt.

Zur sicheren Durchführung von Fernwartungsarbeiten verweise ich auf meine Ausführungen in Abschnitt 20.1.4 meines 14. Tätigkeitsberichts von 1992 und der Orientierungshilfe „Sicherheitsstatus der ISDN-Nebenstellenanlage (mit Musterbeispiel)“.

17.3.10 Projekt „Verdiensterhebung über das Internet“

Als ein positives Beispiel zur Anwendung kryptografischer Verfahren einer staatlichen Dienststelle sei hier das Projekt „Verdiensterhebung über das Internet“ des Bayerischen Landesamtes für Statistik und Datenverarbeitung (LfStaD) genannt.

Im Vollzug des Bundesstatistikgesetzes (BStatG) werden im vierteljährlichen Turnus durch das LfStaD die Daten zu den Einkommen von Angestellten und Arbeitern bei bayernweit ca. 4000 Betrieben erhoben. Diese Erhebung wurde bisher ausschließlich über die Zu- und Rücksendung von Papier-Formularen durchgeführt – eine für beide Seiten aufwendige Vorgehensweise.

Ziel des Projektes ist, den auskunftspflichtigen Betrieben ab Juli 2000 wahlweise zum Papierversand die Möglichkeit der elektronischen Übermittlung der Erhebungsdaten über das Internet anzubieten. Bei dem Online-Verfahren können die auskunftspflichtigen Betriebe über eine Browseroberfläche entweder die Online-Fragebogen wählen und diese manuell ausfüllen oder aus ihrer eigenen EDV entsprechende Dateien erzeugen und diese in den Online-Fragebogen einfügen.

Zur Sicherung der Kommunikation und der Daten gelangen folgende Maßnahmen zur Anwendung:

- Bei Anmeldung am Online-Verfahren wird eine mit SSL abgesicherte Verbindung zwischen dem LfStaD und dem meldepflichtigen Betrieb aufgebaut, wobei der Rechner des LfStaD in automatischer Abstimmung mit dem Browser des Meldepflichtigen zunächst versucht, die derzeit maximal mögliche Schlüssellänge (128 Bit) zu verwenden. Wird dies vom Browser des Meldepflichtigen nicht unterstützt, wird eine kürzere Schlüssellänge von 40/56 Bit benutzt.
- Zur Authentifizierung des LfStaD-Servers dem Browser des meldepflichtigen Betriebes gegenüber wird ein Serverzertifikat benutzt, das sich das LfStaD von einer kommerziellen Zertifizierungseinrichtung hat ausstellen lassen.
- Die für das Verfahren notwendige Identifizierungs- und Authentizitätsprüfung des Betriebes geschieht durch Eingabe der Betriebsnummer und eines sechsstelligen Passwortes. Das für

jeden Betrieb spezifische Passwort wird durch das LfStaD vorgegeben und an einen vorbestimmten Mitarbeiter des Betriebes persönlich auf postalischem Wege übermittelt.

- Die sog. Zulassungsdatei mit den Identitifizierungs- und Authentifizierungsdaten der Meldepflichtigen Betriebe ist auf dem Server des LfStaD mit PGP verschlüsselt abgespeichert und wird nur für die aktuelle Durchführung einer Identifizierungs- und Authentifizierungsprüfung temporär entschlüsselt.
- Bei Eingang am Server des LfStaD werden automatisch die gemachten statistischen Angaben aus den Erhebungsdaten extrahiert und an den zentralen Statistikrechner weitergeleitet.
- Der meldepflichtige Betrieb erhält sofort eine automatische Empfangsbestätigung mit Anzeige der übermittelten Daten, die er ausdrucken und zu seinen Unterlagen nehmen kann.
- Die gesamten Erhebungsdaten werden sodann auf dem Server automatisch mit PGP verschlüsselt, in eine E-Mail gepackt und an die für die Verdiensterhebung zuständige Stelle im LfStaD übertragen.
- Die Entschlüsselung der Erhebungsdaten erfolgt ausschließlich am Arbeitsplatz der für die Verdiensterhebung zuständigen Mitarbeiter und ist aufgrund der asymmetrischen Verschlüsselung nur diesen möglich.

Sowohl über entsprechende Hinweise auf dem Server des LfStaD als auch über die nach wie vor übersandten schriftlichen Unterlagen werden die auskunftspflichtigen Betriebe über die Möglichkeiten der freien Wahl des zu benutzenden Verfahrens, die im Übrigen für jeden Erhebungszeitraum gegeben sind, und die ergriffenen Sicherungsmaßnahmen informiert.

Besonders hervorhebenswert erscheint mir, dass das LfStaD mit diesem Vorhaben bereits im Planungsstadium auf mich mit der Bitte um Beratung zugekommen ist und dass das LfStaD oben genannte Absicherungsmaßnahmen von Anfang an von sich aus vorgeschlagen hat. Ich halte das Projekt aufgrund der pragmatischen Vorgehensweise und der Anwendung von derzeit verfügbaren und im Internet weit verbreiteten Verfahren für ein gelungenes Beispiel dafür, dass auch kryptografische Verfahren rasch, unkompliziert, benutzerfreundlich und für alle Beteiligten nutzbringend eingeführt werden können. Ohne die Verwendung kryptografischer Verfahren wäre dieses Projekt nicht möglich gewesen.

17.4 Orientierungshilfen

Im Berichtszeitraum hat meine Geschäftsstelle drei neue Orientierungshilfen erstellt, die auf meiner Home-Page unter der Rubrik „Technik“ abgerufen werden können. Im Einzelnen handelt es sich um folgende:

- „Veröffentlichungen von Informationen im Internet und im Intranet“
  Durch Unkenntnis über zulässige Informationsinhalte und durch fehlerhafte oder unzureichende technische und organisatorische Maßnahmen ist es möglich, dass bei Veröffentlichung von Informationen auf Web-Servern unberechtigt schutzwürdige Informationen im Internet und im Intranet allgemein zugänglich gemacht werden und so gegen Datenschutzbestimmungen verstoßen wird. Die Orientierungshilfe gibt Hinweise zu möglichen und kritischen Informationsinhalten, aber auch konkrete Tipps für vorbeugende Maßnahmen.

- „Online-Datenschutz-Prinzipien (ODSP)“
  Online-Datenschutz-Prinzipien sind eine umfassende Erklärung zu Grundsätzen und Verfahrensweisen einer Organisation/Einrichtung/Behörde bzgl. der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Informationsangebotes im Internet auftreten. Die ODSP sollen immer dann veröffentlicht werden, wenn personenbezogene Daten online über die Web-Site gesammelt werden. Dies ist dann der Fall, wenn z.B. eine Online-Registrierung verlangt bzw. ermöglicht wird, wenn sonstige Formulare online ausgefüllt werden können oder wenn mittels E-Mail mit der Organisation/Einrichtung/Behörde kommuniziert werden kann. Personenbezogene Daten können aber auch ohne Kenntnis des Besuchers einer Web-Site gesammelt werden, wenn z.B. Cookies oder Protokollierungen verwendet werden. Sammeln Web-Sites nur aggregierte Daten über ihre Besucher, z.B. für Statistiken über Seitenabrufe, oder nur anonymisierte Daten in Form von auf Domain-Ebene reduzierten IP-Adressen, so ist damit keine Speicherung personenbezogener Daten gegeben. Die Veröffentlichung von Online-Datenschutz-Prinzipien ist somit nicht generell nötig. Die Veröffentlichung von ODSP wird jedoch immer empfohlen, weil damit evtl. vorhandene Bedenken und Befürchtungen der „Besucher“ zerstreut werden können. Die Orientierungshilfe gibt eine Hilfestellung zu Rechtsgrundlagen, Inhalt und Veröffentlichung von ODSP.

- „Sicherheitsmaßnahmen im Landkreis-Behördennetz" (Kommunales-Behördennetz)
  Immer mehr Landratsämter beabsichtigen, ein sicheres und leistungsfähiges Intranet für ihre Verwaltungen und für die Kommunen ihres Landkreises zu errichten. Ziele eines solchen Intranets sind beispielsweise der Austausch von E-Mails zwischen den angeschlossenen Stellen, die Nutzung der Internet-Dienste und –Techniken, die Schaffung eines gemeinsamen Informationspools, die zentrale Bereitstellung von Formularen (Formularserver), der zentraler Zugang zum Internet und die Bereitstellung von Online-Diensten für den Bürger. Einem solchen Landkreis-Behördennetz drohen (wie jedem anderen Netz auch) Gefahren, die sowohl von den eigenen Mitarbeitern, als auch von außenstehenden Dritten und von technischen Mängeln ausgehen können. Essenzielle Forderungen an ein solches Netz sind u.a., dass es in sich geschlossen sein muss, dass das Firewall-System von sachverständigen Personen betreut wird und dass alle Verbindungen in das Netz hinein und aus dem Netz heraus ausschließlich über das Firewall-System geführt werden. Die Orientierungshilfe zeigt einige der größten Gefahrenquellen auf und schlägt die Ergreifung entsprechender Sicherheitsmaßnahmen vor.

Die bisherige Orientierungshilfe „Aufgaben eines Benutzerservices" wurde überarbeitet und steht nun mit dem neuen Titel „Einrichten eines Benutzerservices“ ebenfalls auf meiner Home-Page zum Abruf zur Verfügung.

Grundsätzliche Ausführungen und Überlegungen zu moderner Softwareentwicklung und Dokumentation habe ich im gleichnamigen Papier zusammengestellt und in meiner Home-Page veröffentlicht.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat seine Orientierungshilfe „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ mit Stand vom November 2000 überarbeitet.

Neu erstellt wurden vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Orientierungshilfen und Ausarbeitungen:

- „Verzeichnisdienste“

- „Transparente Software – eine Voraussetzung für datenschutzfreundliche Technologien“
- „Behörden im Internet“

18 Der Beirat

Dem Beirat beim Landesbeauftragten für den Datenschutz gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den **Landtag**:

Mitglieder:		Stellvertretende Mitglieder:	
Franz Brosch	CSU	Prof. Dr. Hans Gerhard Stockinger	CSU
Petra Guttenberger	CSU	Johann Neumeier	CSU
Alexander König	CSU	Christian Meißner	CSU
Bernd Sibler	CSU	Thomas Obermeier	CSU
Dr. Klaus Hahnzog	SPD	Harald Güller	SPD
Franz Schindler	SPD	Joachim Wahnschaffe	SPD

Für den **Senat**:

bis 31.12.1999

Wolfgang Burnhauser	Hartwig Reimann

Für die **Staatsregierung**:

Christian P. Wilde	Bayerisches Staatsministerium des Innern	Hubert Kranz	Bayerisches Staatsministeri-um der Finanzen

Für die **Sozialversicherungsträger**:

Dr. Ludwig Bergner	Erster Direktor der LVA Oberbayern	Dr. Helmut Platzer	Vorstandsvorsit-zender der AOK Bayern
ab 01.08.2000: Werner Krempl	Erster Direktor der LVA Oberfranken und Mittelfranken		

Für die **Kommunalen Spitzenverbände**:

Klaus Eichhorn	Gechäftsführender Direktor der AKDB	Wolfgang Kellner	Abteilungsleiter bei der AKDB

Für den **Verband freier Berufe e. V.**:

Erwin Stein	Präsident der Steuerberater-kammer München	Dr. Wolf-Dieter Seher	Zahnarzt
ab 01.05.1999: Margit Bertinger	Steuerberaterin und Wirtschafts-prüferin Präsidiumsmit-glied des Verban-des Freier Berufe in Bayern	ab 01.05.1999: Klaus von Gaffron	Präsidiumsmit-glied des Ver-bandes Freier Berufe in Bayern Vorsitzender des Berufsverbandes Bildender Künstler Bayern

Den Vorsitz im Beirat führte Franz Brosch, MdL, sein Stellvertreter war Dr. Klaus Hahnzog, MdL.

Der Beirat tagte im vergangenen Berichtszeitraum acht Mal. Dabei befasste er sich u. a. mit folgenden Themen:

- Beratung des 19. Tätigkeitsberichtes
- Novellierung des Bayerischen Datenschutzgesetzes
- Berichte von Datenschutzkonferenzen
- Einrichtung eines Virtuellen Datenschutzbüros
- Wahlen über das Internet
- Polizeiliche Videoüberwachung
- DNA-Analyse bei Strafgefangenen auf der Grundlage einer Einwilligung
- Entwurf der Staatsregierung zur Änderung des Bayerischen Polizeiaufgabengesetzes (insbesondere Einführung von Regelspeicherfristen und Schaffung einer Rechtsgrundlage für die „Mitziehautomatik“)

- Unterrichtung der Polizei und des Betroffenen bei Verfahrenseinstellungen nach § 170 Abs. 2 Strafprozessordnung.

Bei einer Informationsveranstaltung des Beirats zum Thema „Virtuelle Kommunikation des Bürgers mit Behörden“ wurden u. a. folgende Themen behandelt:

- Virtuelles Landratsamt und virtuelle Rathäuser im Landkreisbehördennetz
- Virtueller Markplatz Bayern
- Bericht von der Arbeitsgruppe der Datenschutzkonferenz „Datenschutz in Bürgerbüros“
- Elster – Die elektronische Steuererklärung
- Maschinelle Grundbuchführung.

Mit In-Kraft-Treten der Änderung des Bayerischen Datenschutzgesetzes zum 01.12.2000 wird beim Landtag eine Datenschutzkommission gebildet, die an die Stelle des bisherigen Beirats tritt und dessen Aufgabe (Unterstützung des Landesbeauftragten für den Datenschutz) übernimmt. Die Kommission besteht aus 10 Mitgliedern. Der Landtag bestellt sechs Mitglieder aus seiner Mitte nach Maßgabe der Stärke seiner Fraktionen; das d´Hondtsche Verfahren findet Anwendung. Für Fraktionen, die hiernach nicht zum Zuge kommen, kann der Landtag jeweils ein weiteres Mitglied bestellen. Ferner bestellt der Landtag jeweils ein weiteres Mitglied auf Vorschlag der Staatsregierung, der kommunalen Spitzenverbände, des Staatsministeriums für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit aus dem Bereich der gesetzlichen Sozialversicherungsträger und des Verbands freier Berufe e. V. in Bayern. Für jedes Mitglied wird zugleich ein stellvertretendes Mitglied gewählt. Die am 1. Dezember 2000 bestellten Mitglieder des Beirats beim Landesbeauftragten für den Datenschutz nehmen bis zum Ende der 14. Legislaturperiode die Aufgaben eines Mitglieds der Datenschutzkommission nach Art. 33 des Bayerischen

Der Datenschutzkommission beim Landtag gehören folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den **Landtag**:

Mitglieder:		Stellvertretende Mitglieder:	
Franz Brosch	CSU	Prof. Dr. Hans Gerhard Stockinger	CSU
Petra Guttenberger	CSU	Johann Neumeier	CSU
Alexander König	CSU	Christian Meißner	CSU
Bernd Sibler	CSU	Thomas Obermeier	CSU
Dr. Klaus Hahnzog	SPD	Bärbel Narnhammer	SPD
Franz Schindler	SPD	Joachim Wahnschaffe	SPD
Christine Stahl	BÜNDNIS 90 / DIE GRÜNEN	Susanna Tausendfreund	BÜNDNIS 90 / DIE GRÜNEN

Für die **Staatsregierung**:

Christian P. Wilde	Bayerisches Staatsministerium des Innern	Hubert Kranz	Bayerisches Staatsministerium der Finanzen

Für die **Sozialversicherungsträger**:

Werner Krempl	Erster Direktor der LVA Oberfranken und Mittelfranken	Dr. Helmut Platzer	Vorstandsvorsitzender der AOK Bayern

Für die **Kommunalen Spitzenverbände**:

Klaus Eichhorn	Gechäftsführender Direktor der AKDB	Wolfgang Kellner	Abteilungsleiter bei der AKDB

Für den **Verband freier Berufe e. V.**:

Margit Bertinger	Steuerberaterin und Wirtschafts-prüferin Präsidiumsmit-glied des Verban-des Freier Berufe in Bayern	Klaus von Gaffron	Präsidiumsmit-glied des Ver-bandes Freier Berufe in Bayern Vorsitzender des Berufsverbandes Bildender Künstler Bayern

Den Vorsitz in der Kommission führt Franz Brosch, MdL, sein Stellvertreter ist Dr. Klaus Hahnzog, MdL.

Anlage 1: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.1999 zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlaß der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, daß die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, daß alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, daß die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz

hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muß sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlaß für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.
Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, daß diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Anlage 2: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.1999: Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, daß die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.
Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, daß Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.
Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne daß sie dies bemerken, kann deren mißbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, daß Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Anlage 3: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.1999: Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein "Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, daß das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbringung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, daß jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, daß diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muß institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschrän-

kungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.
Notwendig ist nach Auffassung der Konferenz, daß das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Anlage 4: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.1999: Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL ‘98)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL ‘98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, daß der entsprechende Entwurf bisher geheimgehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmelde-

geheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

Anlage 5: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.08.1999: Angemessener Datenschutz auch für Untersuchungsgefangene

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lässt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar

und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z.B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z.B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

Anlage 6: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25.08.1999: „Gesundheitsreform 2000“

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes „Gesundheitsreform 2000“:

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiterreichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit

dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-l0-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

Die zur Begründung besonders angeführten Punkte ,,Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewähr-

leistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern“ vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotenzials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von *5* auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarzimodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Anlage 7: Appell der Datenschutzbeauftragten des Bundes und der Länder: Hoher Datenschutz für Versicherte bei Gesundheitsreform muss gehalten werden!

Das am 4. November 1999 vom Bundestag beschlossene Gesundheitsreformgesetz 2000 enthält mehrere datenschutzrechtliche Verbesserungen gegenüber der bisherigen Rechtslage. Durch das ‚Aufschnüren" des Pakets und die Preisgabe der zustimmungspflichtigen Teile des Gesetzes droht nun, dass diese Verbesserungen nicht umgesetzt werden. Die Datenschutzbeauftragten des Bundes und der Länder Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein fordern die zuständigen gesetzgebenden Körperschaften auf, den entsprechenden -politisch bislang völlig unstreitigen- Gesetzesteil im Bundesrat passieren zu lassen:

Als Folge der Kritik der Datenschutzbeauftragten wurden vom Bundestag die Regelungen zum Umgang mit den Daten der Versicherten in der gesetzlichen Krankenversicherung erheblich verbessert, z.B. durch die Beschränkung der Datenzugriffsrechte innerhalb der Krankenkassen, die Einführung eines Beratungsgeheimnisses oder eine verbesserte Einbeziehung der Patientinnen und Patienten bei bestimmten ärztlichen Datenübermittlungen.

Wegweisend für die Zukunft im Umgang mit Patientendaten ist aber die vorgesehene Pseudonymisierung des gesamten Abrechnungsverfahrens. Damit können die politisch und ökonomisch angestrebten Auswertungen mit medizinischen Daten, die vor allem der Kostenkontrolle dienen, vorgenommen werden, ohne dass hierdurch die Belange des Patientengeheimnisses oder des Datenschutzes verletzt würden. Das bisherige Verfahren würde grundlegend verbessert, weil bei den Krankenkassen auch Krankenhaus- und Arzneimittelkosten nicht mehr personenbezogen abgerechnet werden müssten — die Gefahr des ,,gläsernen Patienten" würde erheblich reduziert.

Dieser versichertenfreundliche Gesetzesteil ist jedoch im Bundesrat zustimmungspflichtig. Während der Beratungen in den Ausschüssen des Bundestages wurde er quer durch die Parteien befürwortet und so verabschiedet. Selbst die Kassen und die Pharmaindustrie begrüßten die Vor-

schläge weitgehend. Bedeutende zusätzliche Kosten würden durch das neue Verfahren nicht entstehen.

Es stünde allen politisch Handelnden gut zu Gesicht, den Datenschutz im besonders schützenswerten Bereich des Gesundheitswesens trotz aller politischer Kontroversen zu verbessern. Wir appellieren daher an die Bundesregierung bzw. das Gesundheitsministerium, die erreichten guten Datenschutzregelungen in den Bundesrat einzubringen, und an den Bundesrat, diesen zuzustimmen.

Anlage 8: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999: Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten läßt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsge-

heimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.
In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.
Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Anlage 9: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999: DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u.a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne richterliche Anordnung - erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z.B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon aus-

zugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Regelung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen.

Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anlage 10: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999: Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 11: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999 zum Beschluß des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anläßlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluß heißt es: "Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".
Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 12: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999: „Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung“

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz Gewähr leistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, sodass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend Gewähr leistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis

gestellt. Richtigerweise wird darin die Kryptographie als "eine entscheidende Voraussetzung für den Datenschutz der Bürger" besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,

- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,

- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,

- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 13: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999: „Täter-Opfer-Ausgleich und Datenschutz“

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.
Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z.B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muss gesetzlich geschützt werden.

Anlage 14: Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999: Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anlage 15: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000: Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o.ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich geprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.

Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.
Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.

Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).
Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.
Damit sind Regelungen z.B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.
Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.

Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.

Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken.

Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.

Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.

Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

Anlage 16: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000: Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,

- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z.B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,

- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,

- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsaus-

schuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anlage 17: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000: Unzulässiger Speicherungsumfang in "INPOL-neu" geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung "INPOL-neu" eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur so weit eingegriffen wird, wie dies im Rahmen der Erforderllichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die "gesamte kriminelle Karriere" jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereitgehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf "Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung". Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die "Straftaten", nicht die einzelne Person und auch nicht das "Gesamtbild einer Person". Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anlage 18: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000: Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

Erhebliche Zunahme der Telekommunikationsvorgänge

Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mail-boxen sowie das Internet genutzt.

Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten

- Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
- Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
- Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
- Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
- Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten

Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

Entwicklung des Internets zum Massenkommunikationsmittel

Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

Schwer durchschaubare Rechtslage

Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: *1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802*

Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.

Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen "ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.

Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseu-donyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.

Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.

Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstelenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselungvon elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deut-

schen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anlage 19: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000: „Data Warehouse, Data Mining und Datenschutz“

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im "Data Warehouse" werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. "Data Mining" bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem "Daten-Lagerhaus" gesammelt werden.

- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.

- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.

- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.

- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten "Daten-Lagerhäusern" rechtswidrig.

- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). "Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von "Data Warehouse"- und "Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anlage 20: Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000: Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,

- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch videotechnisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.
Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.
   - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. (Anmerkung: Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen) *Dafür kommen – **soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen** – unter Anderem in Betracht:*
     - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der*

Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.

- *für die Verkehrslenkung nur Übersichtsaufnahmen,*
- *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*

- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im Einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.

- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das

Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Anlage 21: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26.06.2000: Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufenden parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der

gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff“ ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z.B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn - wie in den „Wire-tap-Reports“ der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe“.

Anlage 22: Entschließung der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2000: Auftragsdatenverarbeitung durch das Bundeskriminalamt

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden. § 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu.
Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.
Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.
Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet.
Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen. Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.
Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung. Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten.

Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln.
Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Anlage 23: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. 10. 2000 zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.
Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des

betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.
Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anlage 24: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. 10. 2000: Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.
Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen.
Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei

gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestim-mung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwir-ken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytischeMethode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten..
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.
7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unver-einbar.

Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwer wiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe. Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können. Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Anlage 25: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. 10. 2000: Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mo-

biltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zugrunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

Anlage 26: Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. 10. 2000: Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung –

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten Gewähr leistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Abkürzungsverzeichnis

Abs.	Absatz
ADO	Allgemeine Dienstordnung
ADV	Automatisierte Datenverarbeitung
AGKRG	Gesetz zur Ausführung des Krebsregistergesetzes
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
AllMBl	Allgemeines Ministerialamtsblatt
Alt.	Alternative
AMD	Arbeitsmedizinischer Dienst
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
API	Application Program Interface
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
ASMK	Konferenz der Ministerinnen und Minister, Senatorinnen und Senatoren für Arbeit und Soziales der Länder
ATG	Aktionsforum Telematik im Gesundheitswesen
AÜG	Arbeitnehmerüberlassungsgesetz
AUGEMA	Automatisiertes gerichtliches Mahnverfahren
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
BAQ	Bayerische Arbeitsgemeinschaft für Qualitätssicherung in der stationären Versorgung
BauGB	Baugesetzbuch
BayArchivG	Bayer. Archivgesetz
BayBesG	Bayerisches Besoldungsgesetz
BayBG	Bayer. Beamtengesetz
BayBO	Bayerische Bauordnung
BayDSG	Bayerisches Datenschutzgesetz
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayGlG	Bayerisches Gleichstellungsgesetz
BayHO	Bayer. Haushaltsordnung
BayKrG	Bayerisches Krankenhausgesetz
BayKRG	Gesetz über das bevölkerungsbezogene Krebsregister Bayern
BayPVG	Bayerisches Personalvertretungsgesetz
BayRDG	Bayerisches Rettungsdienstgesetz
BayVBl	Bayerische Verwaltungblätter
BayVSG	Bayerisches Verfassungschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BDSG	Bundesdatenschutzgesetz
BEG	Bundesentschädigungsgesetz

BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGK	Bayerische Gesundheitschipkarte und Kommunikation
BGSG	Bundesgrenzschutzgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BLKA	Bayerisches Landeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesministerium für Gesundheit
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BÜVO	Beitragsüberwachungsverordnung
BYBN	Bayerisches Behördennetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
CA	Certification Authority
CC	Common Criteria
CD	Compaktdisk
CERT	Computer Emergency Response Team
CHAP	Callenge Authentication Protocol
DAE	Deutsche Arbeitsgemeinschaft für Epidemiologie
DFG	Deutsche Forschungsgemeinschaft
DGSMP	Deutsche Gesellschaft für Sozialmedizin und Prävention
DNA-Analyse	Molekulargenetische Untersuchung
DSRV	Datenstelle der Rentenversicherungsträger
DV	Datenverarbeitung
DVKRG	Verordnung zur Durchführung des Krebsregistergesetzes
EA	Errichtungsanordnung für Dateien
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EG-Datenschutzrichtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
ELSTER	Elektronische Steuererklärung
EStG	Einkommensteuergesetz
EU	Europäische Union
FTAM	File Transfer, Access and Management
G-10-Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz)
GAST-Dateien	Dateien zur Gefahrenabwehr und Strafverfolgung
gem.	Gemäß
GEWAN	Gewerbeanmeldungs-Software

GG	Grundgesetz
GKV	Gesetzliche Krankenversicherung
GLKrWG	Gemeinde- und Landkreiswahlgesetz
GMDS	Deutsche Gesellschaft für medizinische Information, Biometrie und Epidemiologie
GO	Gemeindeordnung
GSM	Global System for Mobile Communications
GVBl.	Gesetz- und Verordnungsblatt
GVG	Gesellschaft für Versicherungswissenschaft und -gestaltung e. V.
HCP-Protokoll	Health Care Professional Protokoll
HTML	Hypertext Markup Language
IBP	Informationssystem der Bayerischen Polizei
IDEA	International Data Encryption Algorithm
IMSI	International Mobile Subscriber Identität
INPOL	Informationssystem der Polizei (bundesweit)
IPv6, IPng	Internet Protocol Version 6, Internet Protocol next generation
ISDN	Integrated Services Digital Network
IT-GSHB	IT-Grundschutzhandbuch
ITSEC	Information Technology Security Evaluation Criteria
IuKDG	Informations- und Kommunikationsdienste-Gesetz
IuK-Systeme	Informations- und Kommunikationssysteme
JuMiG	Justizmitteilungsgesetz
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KBV	Kassenärztliche Bundesvereinigung
KHG	Krankenhausfinanzierungsgesetz
KIS	Krankenhausinformations- und Kommunikationssystem
KORA	Kooperative Gesundheitsforschung in der Region Augsburg
KRG	Krebsregistergesetz des Bundes (bis 31.12.1999)
KVB	Kassenärztliche Vereinigung Bayerns
KVK	Krankenversichertenkarte
KVR	Kreisverwaltungsreferat
KZBV	Kassenzahnärztliche Bundesvereinigung
KZVB	Kassenzahnärztliche Vereinigung Bayerns
LfStaD	Landesamt für Statistik und Datenverarbeitung
LfV	Bayerisches Landesamt für Verfassungsschutz
LHSt.	Landeshauptstadt
LKrO	Landkreisordnung
LMU	Ludwig-Maximilians-Universität München
LT-Drs.	Landtagsdrucksache
LVA	Landesversicherungsanstalt
m.E.	meines Erachtens
MDK	Medizinischer Dienst der Krankenversicherung

MdL	Mitglied des Landtages
MDStV	Mediendienste-Staatsvertrag
MeldeG	Bayerisches Meldegesetz
MiStra	Anordnung über Mitteilungen in Strafsachen
MiZi	Anordnung über Mitteilungen in Zivilsachen
MSC	Mobile Switching Center
MUCK	Multifunktionale Chipkarte
MWG `92	Münchner Weltwirtschaftsgipfel 1992
Nds.	Niedersächsisch
NJW	Neue Juristische Wochenschrift
o.e.	oben erwähnt
o.g.	oben genannt
OSS	Online Service System; SAP-Fernwartung
PAG	Bayerisches Polizeiaufgabengesetz
PC	Personalcomputer
PD	Polizeidirektion
PFAD	Personen- und Fall-Auskunftsdatei
PGP	Pretty Good Privacy
PHW	Personenbezogener Hinweis
PP	Polizeipräsidium
PStG	Personenstandsgesetz
PSV	Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung
PsychThG	Psychotherapeutengesetz
Rdn(r).	Randnummer
RegTP	Regulierungsbehörde für Telekommunikation und Post
RSA/DES	Rivest, Shamir, Adleman/Data Encryption Standard
RV	RV Rentenversicherung
S.	Seite
S/MIME	Secure Multipurpose Internet Mail Extensions
SAP	Systems, Applications, and Products
SDBY	Stastsschutzdatei Bayern
SDÜ	Schengener Durchführungsabkommen
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
SIS	Schengener Informationssystem
SozhiDAV	Sozialhilfedatenabgleichsverordnung
SSL	Secure Sockets Layer
STARIS	Staatsanwaltschaftliches Registrierungs- und Informationssystem
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
StMAS	Bayer. Staatsministerium für Arbeit und Sozialordnung, Familie,

	Frauen und Gesundheit
StPO	Strafprozeßordnung
StVÄG	Strafverfahrensänderungsgesetz
TB	Tätigkeitsbericht
TCP/IP	Transmission Control Protocol/Internet Protocol
TDDSG	Teledienstedatenschutzgesetz
TMSI	Temporary Mobile Subscriber Identity
TOA	Täter-Opfer-Ausgleich
TTP	Trusted Third Parties
TÜ	Telefonüberwachung
u.a.	unter anderem
VBG 100	Unfallverhütungsvorschrift Arbeitsmedizinische Vorsorge
VDR	Verband Deutscher Rentenversicherungsträger
VersammlG	Versammlungsgesetz
VGemO	Verwaltungsgemeinschaftsordnung
VGH	Verwaltungsgerichtshof
vgl.	Vergleiche
ViCLAS	Violent Crime Linkage Analysis System (Analyse-System zur Verknüpfung von Gewaltverbrechen)
VSA	VSA Verrechnungsstelle der Süddeutschen Apotheken GmbH
VwVfG	Verwaltungsverfahrensgesetz
WaffG	Waffengesetz
z.B.	zum Beispiel
ZPO	Zivilprozeßordnung
ZStV	Zentrales staatsanwaltschaftiches Verfahrensregister

Stichwortverzeichnis