20. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

(gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes)

Berichtszeitraum 2001/2002

1 Sicherheit und Datenschutz nach dem 11. September 2001

1.1 Relativierung des Datenschutzes

Das schreckliche Attentat auf die Vereinigten Staaten von Amerika am 11. September 2001 hatte auch erhebliche Folgen für den Datenschutz. Ich meine hier nicht primär den Inhalt des "Ersten" und "Zweiten" Sicherheitspakets sowie die Vorstellungen von Staatsminister Dr. Beckstein für ein "Drittes Sicherheitspaket", sondern die fast intuitiven Aussagen führender Politiker unmittelbar nach dem Attentat und in der weiteren Folge. Das Recht auf informationelle Selbstbestimmung wurde in Frage gestellt ungefähr sinngemäß mit den Worten:

Es muss auch über den Datenschutz grundsätzlich nachgedacht werden.

Ich hoffe nicht, dass in dieser Formulierung ein grundsätzliches Misstrauen gegenüber dem Datenschutz, wenn nicht sogar eine grundsätzliche Ablehnung zum Ausdruck kommt, kann es – vorsichtig gesprochen – aber auch nicht ausschließen. Auf jeden Fall ist der Stellenwert des Datenschutzes im Ansehen der politischen Öffentlichkeit zumindest in Gefahr, wenn nicht gesunken.

Diese Auffassungen sind unberechtigt und sie sind gefährlich: Sie sind unberechtigt, weil Datenschutz auch schon bisher die erforderliche Datenverarbeitung im Sicherheitsbereich nicht verhindert hat. Nach der Rechtsprechung des Bundesverfassungsgerichts kann das "Recht jedes Einzelnen, selbst zu bestimmen, wer was über ihn weiß und was er mit diesem Wissen anfängt", im überwiegenden Interesse der Allgemeinheit eingeschränkt werden. Solche Einschränkungen und damit Datenverarbeitungsmöglichkeiten sind mit den schon bestehenden Sicherheitsgesetzen in vielfacher Weise erfolgt. Insbesondere ist die Zusammenarbeit zwischen Polizei und Verfassungsschutz schon bisher in vielfacher Weise möglich.

Die Forderung nach *"grundsätzlichem Nachdenken über den Datenschutz"* ist aber auch gefährlich, weil sie an den Kern des Grundrechts geht: Sie birgt die Gefahr, dass in die geforderte Abwägung das Grundrecht auf informationelle Selbstbestimmung eben nicht mehr mit

dem Stellenwert eines Grundrechts eingeht, sondern dass es als beliebig fungible Größe angesehen wird, die ebenso beliebig eingeschränkt werden kann.

Bereits kurze Zeit nach den Terroranschlägen in den USA am 11. September 2001 wurde der teilweise undifferenzierte Ruf nach Einschränkung des Datenschutzes und nach diversen Gesetzesänderungen laut. Als sich bei den Ermittlungen in den USA herausstellte, dass einige der Attentäter in Deutschland völlig unauffällig gelebt und die Anschläge hier geplant und vorbereitet hatten, stellte sich die Frage, wie es dazu kommen konnte. Die Tatsache, dass die Attentäter bei ihren Vorbereitungshandlungen nicht aufgefallen waren, wurde als Anzeichen dafür gesehen, dass die zum damaligen Zeitpunkt bestehenden gesetzlichen Möglichkeiten der Behörden offenbar nicht ausreichten. Einige maßgebliche Politiker waren schnell bei der Hand, die angeblichen Defizite ohne nähere Begründung einem ihrer Meinung nach übertriebenen Datenschutz in Deutschland zuzuschreiben und den Datenschutz als hinderlich im Kampf gegen den Terrorismus hinzustellen.

Eine solche Einstellung halte ich wie gesagt für grundfalsch. Die einseitige Betonung der Sicherheit berücksichtigt nicht, dass Datenschutz wesentliche Voraussetzung unseres freiheitlich verfassten Staatswesens ist. Zwar stehen Sicherheit und Datenschutz von jeher in einem Spannungsverhältnis. Dieses kann und muss jedoch jeweils entsprechend der Erforderlichkeit und Verhältnismäßigkeit ausgeglichen werden. Wenn sich nach sorgfältiger Prüfung daher herausstellt, dass eine Gesetzesänderung in diesem Rahmen zum effektiven Kampf gegen den Terrorismus notwendig ist, wird sich auch der Datenschutz dem nicht entziehen. Um dies klarzustellen haben sich die Datenschutzbeauftragten des Bundes und der Länder in zwei Entschließungen zur Terrorismusbekämpfung geäußert und darin hervorgehoben, dass sie zwar den Kampf gegen den Terrorismus mit Nachdruck unterstützen, die Freiheits- und Persönlichkeitsrechte der Einzelnen dabei jedoch angemessen berücksichtigt werden müssen.

1.2 Terrorismusbekämpfungsgesetz

Angesichts des bisher ungeahnten Ausmaßes des internationalen Terrorismus und der völlig neuen Bedrohungssituation verabschiedete der Bundestag innerhalb weniger Monate ein umfangreiches Gesetzespaket mit zahlreichen Erweiterungen der Befugnisse von Sicherheits-

und Ausländerbehörden. Dabei geht es unter anderem um folgende wesentliche Neuregelungen:

- Dem Bundesamt für Verfassungsschutz - sowie den Landesämtern für Verfassungsschutz bei entsprechender landesgesetzlicher Regelung - wird nunmehr ausdrücklich die Befugnis eingeräumt, im Einzelfall zur Erfüllung bestimmter Aufgaben

  - bei Luftfahrtunternehmen unter anderem Auskünfte über Namen, die Inanspruchnahme von Transportleistungen und sonstigen Umständen des Luftverkehrs

  - bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen unter anderem Auskünfte zu Konten, Konteninhabern und Geldbewegungen

  - bei Personen und Unternehmen, die Postdienstleistungen erbringen, Namen, Anschriften, Postfächer und sonstige Umstände des Postverkehrs sowie

  - bei Telekommunikations- und Teleddiensteunternehmen für die Vergangenheit und Zukunft Auskünfte über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten

  einzuholen.

  Neben einer Klarstellung und Erleichterung bereits bestehender Befugnisse wurden durch dieses Gesetzespaket aber auch weitere, völlig neue Befugnisse geschaffen.

- Die Änderung des Pass- bzw. Personalausweisgesetzes lässt es zu, biometrische Merkmale von Fingern, Händen oder Gesicht in diese Ausweisdokumente aufzunehmen. Die Arten der biometrischen Merkmale, Einzelheiten dazu und zur Verschlüsselung sowie die Art der Speicherung, Verarbeitung und Nutzung sollen durch ein gesondertes Bundesgesetz geregelt werden.

- Im Bereich des Ausländerrechts zielen diverse Änderungen auf eine Verbesserung des Informationsaustausches zwischen Sicherheitsbehörden und Ausländerbehörden bzw.

Auslandsvertretungen. Darüber hinaus wurden neue identitätssichernde Maßnahmen eingeführt und die Kontrolle von einreisenden Ausländern verschärft, um damit möglichen Sicherheitsrisiken zu begegnen.

- Das Bundeskriminalamt kann nunmehr zur Erfüllung seiner Aufgaben als Zentralstelle Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung unmittelbar durch Anfragen bei öffentlichen oder nichtöffentlichen Stellen erheben und ist damit nicht mehr auf die vorrangige Anfrage bei den Polizeien des Bundes und der Länder angewiesen.

- Durch Änderung des Sozialgesetzbuchs ist nun auch eine Übermittlung von bestimmten Sozialdaten zur Durchführung einer Rasterfahndung zulässig.

U.a. durch den Einsatz der Datenschutzbeauftragten wurden beim Erlass des Terrorismusbekämpfungsgesetzes aber auch wesentliche Forderungen des Datenschutzes berücksichtigt:

- Die Geltung zahlreicher Änderungen ist auf fünf Jahre beschränkt, außerdem sind sie vor Ablauf dieser Frist zu evaluieren.

- Die Auskunftsrechte des Bundesamts für Verfassungsschutz - und entsprechend diejenigen der Landesämter für Verfassungsschutz - wurden strengen Verfahrensvorschriften unterworfen.

- Die Einrichtung einer bundesweiten Zentraldatei für biometrische Merkmale wurde ausdrücklich gesetzlich ausgeschlossen.

- Im Rahmen einer Rasterfahndung dürfen Gesundheitsdaten von den Sozialbehörden nicht an die Polizei übermittelt werden.

- Dem Bundeskriminalamt wurde entgegen ursprünglicher Planungen nicht die Befugnis eingeräumt, Vorermittlungen ohne Anfangsverdacht im Sinne der Strafprozessordnung durchzuführen.

1.3 Gesetzgeberische Folgerungen in Bayern

In Bayern wird im Landtag inzwischen ein Regierungsentwurf behandelt, in dem die durch das Terrorismusbekämpfungsgesetz geschaffenen Befugnisse der Sicherheitsbehörden in Landesrecht umgesetzt und erweitert werden. Anders als dem Bundesamt für Verfassungsschutz sollen dem Landesamt für Verfassungsschutz die oben genannten Auskunftsbefugnisse auch zur Bekämpfung des gewaltbereiten Inlandsextremismus und der organisierten Kriminalität zustehen.

Bestrebungen gegen die Organisierte Kriminalität im Geltungsbereich des Grundgesetzes haben grundsätzlich keinen Bezug zum Terrorismus, so dass die Ausdehnung der Auskunftsrechte hierauf weder erforderlich noch verhältnismäßig ist. Außerdem ist der Begriff der Organisierten Kriminalität derart weit gefasst, dass die Gefahr einer zu weitgehenden Anwendung der Befugnisse besteht. Ich habe mich deshalb gegen Erweiterungen in diesem Umfang ausgesprochen.

Gegen die uneingeschränkte Erweiterung der Befugnisse auf den Inlandsextremismus spricht u.a., dass im Gesetzentwurf lediglich vorausgesetzt wird, dass die dort genannten Schutzgüter durch Anwendung von Gewalt oder darauf ausgerichtete Vorbereitungshandlungen gefährdet werden; damit würden z.B. auch einfache Sachbeschädigungen erfasst werden, was ich für zu weitgehend halte.

Des Weiteren habe ich mich dafür ausgesprochen, dass personenbezogene Informationen, die aus Eingriffen in den Schutzbereich des Art. 13 GG („großer Lauschangriff“) gewonnen wurden, eine Pflicht zur Kennzeichnung eingeführt wird. Eine solche Verpflichtung hatte das Bundesverfassungsgericht in seinem Urteil zur strategischen Fernmeldeüberwachung (NJW 2000, 55, 57, 64) für personenbezogene Daten aus Telefonüberwachungen ausgesprochen. Nur so könne die Zweckbindung und die besonderen Verwendungsbeschränkungen dieser sensiblen Daten eingehalten und überwacht werden.

Das gleiche muss nach meiner Auffassung für Daten gelten, die aus der Wohnraumüberwachung gewonnen werden. Diese greift mindestens so tief in die private Kommunikation ein wie die Telefonüberwachung. Nach meiner Auffassung ist im Gegenteil der Eingriff noch

tiefer, weil das Grundrecht auf Unverletzlichkeit der Wohnung den engsten Privatbereich des Menschen schützt. Innerhalb der Mauern seiner Wohnung soll der Mensch vor Eingriffen sicher sein. Das besagt Art. 13 Abs. 1 des GG: Die Wohnung ist unverletzlich.

Die Grundsätze zur Telefonüberwachung müssen deshalb nach meiner Auffassung um so mehr auf die Überwachung von Wohnräumen angewendet werden.

1.4 Weitere Initiativen im Bayerischen Landtag

Über diese Regelungen hinaus hat die CSU-Landtagsfraktion Anträge eingebracht, die auf eine weitere Verschärfung der Sicherheitsgesetze abzielen. Ich habe zu jedem einzelnen dieser Anträge Stellung genommen und dabei meine Bedenken in datenschutzrechtlicher Hinsicht dargelegt. Auf einzelne Forderungen gehe ich im Folgenden ein:

- Eine für die Einbürgerungsbehörden bundesweit zwingend vorgeschriebene Regelanfrage beim Verfassungsschutz vor einer Einbürgerung sowie vor Erteilung einer unbefristeten Aufenthaltserlaubnis oder einer Aufenthaltsberechtigung soll eingeführt werden.
  Gegen eine entsprechende Regelanfrage vor einer Einbürgerung habe ich keine Bedenken erhoben. Sie wird in Bayern bereits praktiziert. Die Regelanfrage vor einer unbefristeten Aufenthaltserlaubnis oder einer Aufenthaltsberechtigung habe ich jedenfalls für eine Herkunft aus Gefährderstaaten nicht grundsätzlich abgelehnt, da diese ebenfalls langfristige feste Aufenthaltstitel geben; ich habe jedoch darauf hingewiesen, dass im Unterschied zur Einbürgerung hier keine vollendeten Tatsachen geschaffen werden und der Ausländer auch danach noch ausgewiesen werden kann.

- Die durch das Terrorismusbekämpfungsgesetz festgelegten strengen Verfahrensvoraussetzungen für die Informationserhebungsbefugnisse des Landesamts für Verfassungsschutz bei Kreditinstituten, Finanzdienstleistern, Postdienstleistern und Luftfahrtunternehmen sollen aufgehoben werden.
  Diese Vorschriften über das Verfahren zur Auskunftseinholung und die Kontrolle der Maßnahmen tragen der Intensität des Eingriffs Rechnung und sollten daher aufrecht er-

halten bleiben. Auf meine Hinweise hin wurden in der Beratung der Anträge im Innenausschuss des Bayerischen Landtags die Postdienstleister von der beantragten Erleichterung ausgenommen. Diese Änderung begrüße ich im Hinblick auf das Brief-, Post- und Fernmeldegeheimnis in Art. 10 GG.

- Im Ausländerzentralregister soll die Religions- und die ethnische Zugehörigkeit eines Ausländers verpflichtend, zumindest jedoch bei freiwilliger Angabe, gespeichert werden.
  Nach dem Grundgesetz ist die Erhebung und Speicherung der Religionszugehörigkeit nur dann zulässig, wenn von der Zugehörigkeit zu einer Religionsgemeinschaft Rechte und Pflichten abhängen oder den Erfordernissen einer gesetzlich angeordneten statistischen Erhebung entsprochen wird. Eine verpflichtende Angabe wäre daher grundgesetzwidrig. Die Möglichkeit, freiwillig gemachte Angaben zur Religionszugehörigkeit zu speichern, ist bereits durch das Terrorismusbekämpfungsgesetz eingeführt worden.

- Entgegen der ausdrücklichen Regelung des Bundesgesetzgebers im Terrorismusbekämpfungsgesetz soll eine bundesweite Zentraldatei, in der die biometrischen Daten, die in Pässen und Personalausweisen aufgenommen werden sollen, errichtet werden. Eine solche, alle Bundesbürger umfassende Referenzdatei birgt ein sehr hohes Missbrauchspotential. Ich lehne sie daher entschieden ab.

- Der Straftatenkatalog für eine akustische Wohnraumüberwachung soll erweitert und die zeitliche Befristung verlängert werden. Darüber hinaus soll eine optische Wohnraumüberwachung eingeführt werden.
  Im Hinblick auf das Grundrecht der Unverletzlichkeit der Wohnung sind diese empfindlichen Eingriffe eng zu fassen, so dass ich die immer wiederkehrenden Forderungen nach einer erneuten Erweiterung des ohnehin bereits umfangreichen Straftatenkatalogs für eine akustische Wohnraumüberwachung jedenfalls ohne ausreichende Erfolgskontrolle der bisherigen Maßnahmen ablehne. Für eine Verlängerung der Befristung der Dauer einer akustischen Wohnraumüberwachung sehe ich keine Erforderlichkeit. Eine optische Wohnraumüberwachung würde in unzulässiger Weise in den Wesensgehalt des Grundrechts nach Art. 13 GG eingreifen. Sie ist deshalb uneingeschränkt abzulehnen.

Angesichts der dargestellten Entwicklung, die sich auch noch 1 Jahr nach den Anschlägen fortsetzt, wie dies die jüngsten schrecklichen Anschläge auf Bali möglicherweise zeigen, ist damit zu rechnen, dass auch künftig Forderungen nach Verschärfung von Sicherheitsgesetzen erhoben werden.

Wachsamkeit in der Zukunft ist notwendig, dass geplante Gesetzesänderungen nicht unverhältnismäßig in die Freiheits- und Datenschutzrechte der Bürger eingreifen.

2 Überblick

2.1 Übersicht über einige wesentliche Punkte im Berichtszeitraum – positiv und negativ

2.1.1 Polizeibereich

Teilweise umgesetzt wurden die Verbesserungen bezüglich der Datenspeicherungen im Kriminalaktennachweis, über die ich zuletzt (19. TB) berichtet hatte. Ein Hauptkritikpunkt war, dass entlastende Erkenntnisse aus weiteren Ermittlungen nicht ausreichend berücksichtigt wurden. So soll jetzt eine Prüfung der Speicherfrist nicht nur bei Aufnahme eines Ermittlungsverfahrens, sondern auch nach dessen Abschluss erfolgen, damit entlastende Erkenntnisse ebenso berücksichtigt werden können. Meine Forderung nach einem besonderen Hinweis, dass auch das "Ob" der Speicherung nochmals gesondert geprüft werden soll, wurde leider nicht aufgegriffen; ein solcher Hinweis sei wegen des allgemeinen Erforderlichkeitsgrundsatzes entbehrlich. Dagegen halte ich aus meiner Prüfungspraxis einen solchen konkreten Hinweis durchaus für angebracht, wie mehrere Beanstandungen (Nr. 6.1), aber auch Löschungen nach Aufforderung zeigen (Nrn. 6.4 und 6.5).

Erhebliche Ausweitungstendenzen sehe ich im Bereich der Speicherungen im Zusammenhang mit extremistischer Gewalt. So können auch sog. "sonstige Personen" gespeichert werden,

von denen lediglich die Personalien festgestellt wurden, wenn "Tatsachen die Annahme rechtfertigen", dass diese sich in Zukunft an "politisch motivierten Straftaten von erhebliche Bedeutung" beteiligen. Welche Tatsachen sollen das sein? Die Prüfung von Speicherungen in diesem Bereich wird im nächsten Berichtszeitpunkt ein Schwerpunkt sein (Nr. 6.7).

Die Rasterfahndung durch das Bayerische Landeskriminalamt nach dem 11.September hat bis jetzt nur insoweit zu wesentlicher Kritik Anlass gegeben, als die Datei " Rasterfahndung BAO-USA ", in der sämtliche angefallene Daten gespeichert sind, auch nach Durchführung des Datenabgleichs und damit nach Abschluss der Rasterfahndung zwar gesperrt, aber gleichwohl für eventuelle zukünftige Rasterungen weiter vorgehalten wird. Diese Vorratsdatenspeicherung ist vom Gesetz nicht gedeckt, ich habe deshalb unverzügliche Löschung gefordert. Das Innenministerium lehnt sie ab. Dagegen wurden richtigerweise die Personen gelöscht, die dem Grundraster nicht unterfielen (Nr. 6.11).

DNA – Untersuchungen dürfen nach den Vorschriften der Strafprozessordnung nur durchgeführt werden, wenn ein Richter das angeordnet hat. In Bayern wird vielfach eine richterliche Anordnung nicht eingeholt, wenn der Betroffene sich mit der Untersuchung einverstanden erklärt hat. Von einer Beanstandung habe ich im Hinblick auf die schwankende Rechtsprechung – einige Entscheidungen halten eine Untersuchung auf der Grundlage einer Einwilligung für zulässig, andere nicht – abgesehen.

Auf Grund meiner Forderungen wurden aber die Formblätter zur Einwilligungserklärung wesentlich verbessert: Ausführliche Hinweise auf die gesetzliche Lage und die Folgen einer Einwilligung, nämlich den Verzicht auf die richterliche Überprüfung, ausreichende Überlegensfrist auch für Gefangene, keine Bezeichnung des Anschreibens als "Vorladung" (Nr. 6.12.2).

Nicht hinzunehmen ist dagegen, dass auch im Maßregelvollzug grundsätzlich mit "Einwilligungen" gearbeitet wird. Dort sind vielfach erhebliche Zweifel daran angebracht, dass die Betroffenen die Tragweite ihrer Entscheidung richtig abschätzen können. Ich habe deshalb das Staatsministerium des Innern aufgefordert, in diesem Bereich DNA-Analysen nur auf Grund richterlicher Anordnungen durchzuführen und eine Beanstandung angedroht. Das Staatsministerium hat meiner Forderung inzwischen im Grundsatz entsprochen, läßt aber im-

mer noch die Möglichkeit der freiwilligen Einverständniserklärung offen unter der Voraussetzung, dass ein ärztliches Gutachten die Einsichtsfähigkeit bestätigt. Das ist eine Verbesserung. Der sauberste Weg wäre für mich gleichwohl, im Maßregelvollzug immer eine richterliche Entscheidung einzuholen (Nr. 6.12.3).

Ein Ärgernis ist auch der von mir seit langem kritisierte "datenschutzrechtliche Hinweis" auf einem Formblatt der Polizei, mit dem sie die Einwilligung erholt zur Erhebung besonders sensibler Daten z.B. Krankenhaus, Arzt, Finanzamt von Geschädigten, Zeugen, aber auch von Beschuldigten. Der Hinweis vermittelt den Eindruck, dass ansonsten die Befugnis ohne weiteres per richterlicher Anordnung durchgesetzt werden kann. Das ist angesichts strenger gesetzlicher Voraussetzungen durchaus nicht immer der Fall. Die Polizei wäre zu einer Änderung bereit gewesen, das Innenministerium hat das nicht zugelassen. Auch hier prüfe ich eine Beanstandung (Nr. 6.18).

Zur Videoüberwachung öffentlicher Plätze habe ich eine Befugnis im Polizeiaufgabengesetz gefordert. Diese wurde inzwischen in Gestalt des neuen Art. 32 Abs. 2 PAG geschaffen. Kritisiert habe ich die meiner Meinung nach zu lange Speicherfrist (maximal 2 Monate), die Möglichkeit von Tonaufnahmen und die im Zusammenhang mit den Richtlinien zu weitgehende Situierungsmöglichkeit (an jedem Platz, an dem Straftaten begangen wurden oder an dem damit zu rechnen ist). Das würde für jeden belebten Platz im Zentrum großer Städte gelten, was zu einer flächendeckenden Überwachung von Innenstadtbereichen führen könnte. Wie ich in meinem 19. TB (Nr. 5.6.4) ausgeführt habe, hielte ich das wegen des damit verbundenen ständigen Anpassungsdrucks für unzulässig.

Tatsächlich hat sich das Innenministerium und mit ihm die Polizei bei der Errichtung neuer Videoanlagen bis jetzt auf Plätze beschränkt, bei denen wegen des dort eindeutigen erhöhten Strafaufkommens nicht mit einer Ausweitung auf ganze Innenstadtbereiche zu rechnen ist: Auf dem Münchner Oktoberfest wurden neun Kameras installiert, die Nürnberger Polizei hat im Bereich vor dem Bahnhof zwei fest montierte, aber nicht verdrahtete ("Mobile") Kameras situiert. Auf dem Oktoberfest wurde erst auf meine Anforderung auf die Kameras durch Beschilderung hingewiesen, die Aufnahmen sollen im Hinblick auf das internationale Publikum erst nach zwei Monaten gelöscht werden. Diese Frist erscheint mir sehr lange. Auf der anderen Seite muss ich einräumen, dass u.a. im Hinblick auf gewisse internationale Postlaufzeiten

so späte Anzeigen durchaus denkbar sind. Wichtig ist, dass Zugriffe protokolliert werden. Hierauf habe ich hingewiesen. In Nürnberg wird auf die Beobachtung durch Schilder hingewiesen, zu begrüßen ist die kurze Speicherfrist von 7 Tagen. Tonaufzeichnungen erfolgen in beiden Fällen nicht (Nr. 6.13).

Eine Video-Aufnahmen - Sequenz bei Versammlungen musste ich förmlich beanstanden (Nr. 6.14). Gelegentlich einer NPD-Versammlung in München hatte die Polizei friedliche Gegendemonstranten ("Zeigen Sie die rote Karte gegen rechts") sowie Passanten ausführlich videographiert. Diese Aufnahmen waren weder als Übersichtsaufnahmen, noch zur Gefahrenabwehr, noch aus Strafverfolgungsgründen gerechtfertigt. Der Vorgang ist umso bemerkenswerter, als ich im letzten Tätigkeitsbericht ausführlich über die Voraussetzungen von Aufnahmen bei Versammlungen referiert habe (19. TB Nr. 5.6.3).

Die Technik hält auch in weiteren Bereichen der polizeilichen Arbeit Einzug. Dem steht der Datenschutzbeauftragte nicht grundsätzlich negativ gegenüber. Meine Aufgabe ist es aber, auf das Einhalten der gesetzlichen Grenzen, bzw. auf das Vorliegen einer gesetzlichen Befugnis zu achten. Aus dieser Sicht musste ich den probeweise eingeführten automatischen Abgleich der Nummern aller vorbeifahrenden KFZ an einem Grenzübergang kritisch kommentieren. Hierfür gibt es derzeit keine Rechtsgrundlage. Der vom Innenministerium herangezogene Art. 13 PAG ermöglicht nur Stichproben im Einzelfall, nicht aber den lückenlosen Abgleich. Hierfür wäre eine Gesetzesänderung erforderlich. (Nr. 6.15).

2.1.2 Verfassungsschutz

Meine Prüfungen beim Verfassungsschutz haben wie in den Vorjahren wieder im allgemeinen datenschutzgerechtes Arbeiten ergeben.

Wesentliche Kritik muss ich in einem allerdings grundsätzlichem Problembereich anmelden: Das LfV hat im Zuge der Maßnahmen nach dem 11. September auf Ersuchen des Landeskriminalamtes, aber auch im eigenen Interesse, von verschiedenen Stellen die Datenbestände aller Personen, die bestimmte Kriterien erfüllen, erhoben und anschließend zum Teil maschinell mit eigenen Datenbeständen abgeglichen. Diese Maßnahme stellt eine Rasterfahndung

dar, für die das LfV im Gegensatz zur Polizei keine Befugnis hat. Auf die vom LfV geltend gemachte anfänglich fehlende Absicht zum maschinellen Abgleich kann es angesichts des engen zeitlichen Zusammenhangs zwischen Datenerhebung und Abgleich – ein bis zwei Monate - nicht ankommen. Die Maßnahme war deshalb unzulässig. Ich habe den Vorgang wegen seiner grundsätzlichen Bedeutung beanstandet (Nr. 7.1) und die Löschung der durch die Rasterung gewonnenen Erkenntnisse gefordert.

2.1.3 Gerichte und Strafverfolgung und Strafvollzug

Im Gerichtsbereich beschäftigte ich mich u.a. mit der Veröffentlichung von Insolvenzdaten im Internet – Anregungen der Datenschutzbeauftragten wurden vom Bundesgesetzgeber mit einer Verordnungsermächtigung aufgegriffen (Nr. 8.1.1), der Anordnung über Mitteilungen in Zivilsachen – auch hier wurden Forderungen der Datenschutzbeauftragten berücksichtigt (Nr. 8.1.2) und den Aufbewahrungsbestimmungen in verschiedenen Gerichtszweigen, wobei auch hier einzelne Anregungen meinerseits übernommen wurden (Nr. 8.1.3).

Hier hervorheben möchte ich aus den Bereichen strafrechtliche Ermittlungen und Strafvollzug folgende Punkte:

Einem Betroffenen ohne Rechtsanwalt wurde Einsicht in Ermittlungsakten verweigert, obwohl das Strafverfahren durch rechtskräftigen Strafbefehl abgeschlossen war. Dieses Recht auf Akteneinsicht stand dem Betroffenen auch ohne Rechtsanwalt zu, obwohl zum damaligen Zeitpunkt die Strafprozessordnung dazu keine ausdrückliche Regelung enthielt. Das Auskunftsrecht ist wesentlicher Bestandteil des Rechts auf informationelle Selbstbestimmung, nur es gewährleistet das Recht zu wissen, wer, was, wann über jemand weiß und was mit diesem Wissen veranlasst wird. Nur auf der Grundlage solcher Informationen ist eine sachgerechte Rechtsverfolgung möglich. Die Verweigerung der Akteneinsicht zeugt deshalb von einem grundlegenden Missverständnis des Rechts auf informationelle Selbstbestimmung (Nr. 8.2.1.1).

Auch im Fall einer Anfrage des Betroffenen, ob dem Generalstaatsanwalt über das ihn betreffende Verfahren berichtet wurde, musste ich die Verweigerung der Auskunft rügen. Die In-

formation des "Generals" stellt eine Datenübermittlung dar, zu der grundsätzlich Auskunft zu erteilen ist. Das Justizministerium hat diese Auffassung bestätigt (Nr. 8.2.1.2).

Eingesetzt habe ich mich, auch als Vorsitzender des Arbeitskreises Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, für eine datenschutzfreundliche Gestaltung staatsanwaltschaftlicher Informationssysteme. Viele Vorschläge wurden übernommen, es bleiben jedoch Defizite: So wird eine Sperrung (Zugang nur noch für einen sehr eng begrenzten Kreis anstatt aller Mitarbeiter einer Staatsanwaltschaft) abgelehnt von Daten Strafunmündiger, von Opfern von Sexualdelikten und von Mitbeschuldigten, deren Unschuld ausdrücklich festgestellt wurde. Weiter wurde ich von gravierenden Verlängerungen von Speicherfristen, die ich für nicht erforderlich halte, nicht informiert (Nr. 8.2.5).

Ein Schwerpunkt meiner Arbeit im Bereich der Justiz war auch die Datenverarbeitung in Justizvollzugsanstalten. U.a. habe ich mich im Hinblick auf das vom Bundesverfassungsgericht auch in diesem Zusammenhang besonders herausgestellte Brief- und Postgeheimnis gegen eine generelle Briefkontrolle in nahezu allen Justizvollzugsanstalten gewandt, allerdings ohne Erfolg (Nr. 8.3.1). Ich habe die Voraussetzungen dargelegt, unter denen Gefangene Einsicht in "ihren" Gefangenenpersonalakt verlangen können (Nr. 8.3.2). Ich habe gegenüber dem Staatsministerium der Justiz die Grenzen der Offenbarungsmöglichkeiten besonders geschützter ärztlicher Daten gegenüber der Anstaltsleitung aufgezeigt (Nr. 8.3.5.1). Eingesetzt habe ich mich auch für eine gesonderte Aufbewahrung besonders sensibler Daten, wie ärztliche Gutachten und Erkenntnisse aus der Besucherüberprüfung
Das Justizministerium hat auch dies abgelehnt, da dies vom Gesetzgeber nicht vorgeschrieben sei und alle Bediensteten zur Behandlung des Gefangenen aufgerufen seien (Nr. 8.3.5.2).

2.1.4 Kommunales und Meldewesen

Abgesehen von den Projekten zu Einführung von e-government, über die ich an anderer Stelle berichte (Nr. 17.1.2), hat die Nutzung des Internet im kommunalen Bereich auch im Berichtszeitraum wieder Fragen aufgeworfen. Nachstehende hebe ich hier hervor:

Quasi als ersten Schritt zum "electronic voting" kann der Wahlschein nunmehr auch per e-mail oder durch das web beantragt werden (ob weitere Schritte realisierbar sind, bleibt aus meiner Sicht im Hinblick auf das Wahlgeheimnis abzuwarten). Ich habe das Staatsministerium des Innern aufgefordert, bei den Gemeinden darauf hin zu wirken, dass bei Verwendung von "Internet-Formularen" auf die Unsicherheiten des Netzes hingewiesen wird und dass standardmäßig SSL-Verschlüsselung angeboten wird. Das Innenministerium hat die Kommunen entsprechend unterrichtet (Nr. 9.3).

Ein Thema war auch die Veröffentlichung von Sitzungsvorlagen im Internet. Diese Vorlagen dienen der Sitzungsvorbereitung der Ratsmitglieder. Die Daten von Personen in diesen Unterlagen sind nicht für die Öffentlichkeit bestimmt. Eine Veröffentlichung dieser Unterlagen im Netz kommt deshalb aus datenschutzrechtlicher Sicht überhaupt nur in Betracht, wenn sämtliche personenbezogenen Angaben aus den Unterlagen entfernt werden. Dazu zählen auch solche, aus denen auf bestimmte Personen geschlossen werden kann. Die "Bereinigung" der Unterlagen wird deshalb mit hohem Aufwand verbunden sein und wird in vielen Fällen unsicher sein. Das Staatsministerium des Innern rät deshalb und aus weiteren Gründen generell von einer Veröffentlichung dieser Unterlagen im Netz ab. Dieser Empfehlung schließe ich mich an (Nr. 9.4).

Auch auf anderem Feld wirft die technische Entwicklung datenschutzrechtliche Fragen auf: Viele Bürger bewegt die Sorge über schädliche Auswirkungen von Mobilfunk-Sendeanlagen. Städte werden deswegen mit Anfragen nach Standorten überhäuft. Einige Städte gehen deswegen dazu über, diese Standorte im Netz zu veröffentlichen. Eine klare gesetzliche Grundlage dafür fehlt bisher. Wir haben deswegen auf der jüngsten Datenschutzkonferenz auf diese Lücke hingewiesen und eine bundesgesetzliche Regelung gefordert (Anlage 24). Ich habe der Veröffentlichung von sichtbaren Standorten ohne Namen und sonstige persönliche Angaben des Grundstückseigentümers durch kreisfreie Städte nicht widersprochen, da die Anlage ohnehin gesehen werden kann und jedermann nach dem Umweltinformationsgesetz und den dazu erlassenen Ausführungsbestimmungen Anspruch auf Auskunft zu diesen Anlagen hat. Wegen der Offenkundigkeit solcher Anlagen sehe ich auch keine Gründe, die vom Grundstückseigentümer gegen eine solche Auskunft geltend gemacht werden könnten. Ich weise aber ausdrücklich darauf hin, dass das alles nur für sichtbare Anlagen gilt, und dass bezüglich

der Veröffentlichung im Internet die Rechtslage mangels einer ausdrücklichen gesetzlichen Befugnisnorm nicht gesichert ist (Nr. 11.1).

Beanstanden musste ich die Veröffentlichung personenbezogener Daten eines Bürgers in einem straßenrechtlichen Planfeststellungsverfahren. Die Behörde hatte unter Namensnennung Ausführungen zu den wirtschaftlichen Verhältnissen des Betroffenen gemacht. Wie schon das Bundesverfassungsgericht ausführte, ist wegen der Möglichkeit der Vergabe von Betriebsnummern eine Namensnennung nicht erforderlich (Nr. 9.7).

Schließlich hat mich wie in der Vergangenheit die Nutzung des Melderegisters auch wieder beschäftigt. Das Meldegesetz sieht die Möglichkeit vor, dass Parteien und Wählervereinigungen sechs Monate vor allgemeinen Wahlen bestimmte Wählerdaten erhalten, wozu unter anderem nicht das Geburtsdatum gehört. Viele Wähler stehen eine solchen Auskunft negativ gegenüber, sie können deswegen einer Auskunftserteilung bei der Meldebehörde widersprechen. In einigen Fällen wurde dieses einschränkende Verfahren nicht beachtet – es wurden auch Geburtsdaten weitergegeben –, ich musste deshalb Beanstandungen aussprechen (Nr. 10.3).

Nicht immer ist die Datenübermittlung unzulässig: Der Rundfunk hat ein legitimes Recht auf seine Gebühren. Die Meldebehörden sind deswegen nach dem Bayerischen Meldegesetz und der Meldedaten-Übermittlungs-Verordnung befugt, u.a. bei An- und Abmeldungen die Anschrift der volljährigen Einwohner zu übermitteln. Bürger, die hier den Datenschutz zu Hilfe gerufen haben, musste ich deshalb enttäuschen (Nr. 10.4).

2.1.5 Steuerverwaltung

Aus dem Feld der Steuerverwaltung hebe ich hervor, dass für die Teilnahme am Verfahren „Elektronische Lohnsteuerkarte“ („ElsterLohn“) das freiwillige Einverständnis des Arbeitnehmers erforderlich ist (Nr. 12.2).

Weiter habe ich die Finanzverwaltung auf die Problematik hingewiesen, die durch die Angabe der Steuernummer auf den Freistellungsbescheinigungen im Zusammenhang mit der sog.

Bauleistungssteuer und durch Pflicht zur Angabe der Steuernummer auf Rechnungen nach der Neufassung des § 14 UStG entsteht. Es besteht die Gefahr, dass Dritte mit Kenntnis dieser Steuernummer die Möglichkeit erhalten, von den Finanzbehörden Steuerinformationen der Betroffenen zu bekommen (Nr. 12.3).

Daneben erhielt ich durch Eingabe Kenntnis von verschiedenen Verfahrensmängeln, die die Durchbrechung des Steuergeheimnisses zur Folge hatte. Die Finanzbehörden stellten dies nach Hinweisen durch mich ab (Nrn. 12.6 und 12.7).

2.1.6 Personalwesen

Zur Datenverarbeitung im Personalaktenbereich wurde ich im wesentlichen beratend tätig. Schwerpunkte waren die Verarbeitung und Nutzung von Personalaktendaten durch Übersichten über Abwesenheiten (Nr. 13.1.2) – keine Angabe von Gründen - und durch Zeiterfassungsdaten (Nr. 13.1.3) – auch hier keine Angabe von Gründen - , in Intranet und Internet (Nr. 13.1.4) – grundsätzlich Einwilligung erforderlich, außer bei offenkundigen Daten von Funktionsträgern -, in der Rechnungsprüfung (Nrn. 13.2.1 – 13.2.3) – Weiterleitung nur soweit für Zwecke der Rechnungsprüfung erforderlich - , schließlich mit der Erfassung von Daten von Berufsgeheimnisträgern (Nr. 13.3.2) – Aufzeichnung nur der Leistungsentgelte, nicht des Gesprächspartners - und mit Informations- und Einsichtsrechten der Personalvertretung (Nr. 13.4) – Einsicht nur, soweit für die Erfüllung bestimmter Aufgaben erforderlich.

2.1.7 Gesundheitswesen

Im Bereich Gesundheitswesen haben mich unter anderem folgende Themen beschäftigt:

Die Entschlüsselung des menschlichen Genoms hat auch grundlegende Folgen für das Recht auf informationelle Selbstbestimmung. Eine Arbeitsgruppe der Datenschutzkonferenz unter der Leitung meines Hamburger Kollegen, in der ich mitgearbeitet habe, hat Grundsätze für ein "Gendatenschutzgesetz" erarbeitet. Unter anderen wird ein strafbewehrtes Benachteiligungs-

verbot für den Fall gefordert, dass eine genetische Untersuchung abgelehnt wird. Weiter wird verlangt, dass das "Recht auf Nichtwissen" sichergestellt wird (Nr. 4.1).

Ich habe mich an der Diskussion zur Verstärkung der Patientenrechte auf Einsicht in die sie betreffenden ärztlichen Unterlagen sowie zur Verbesserung von Patienten-Informationssystemen beteiligt. Bei den Einsichtsrechten sollen bisherige Begrenzungen – Beschränkung bei sog. subjektiven Wertungen der Ärzte und bei Unterlagen der Psychiatrie – abgebaut werden, bei Patienten-Informationssystemen werden Kriterien zur Verbesserung der Qualität aufgestellt (Nr. 4.2).

In der fortwährenden Diskussion um die Einführung einer Gesundheitskarte mit medizinischen Informationen haben wir gefordert, dass die Patientenrechte auf freie Entscheidung, ob und welche Informationen sie ihrem Arzt zugänglich machen, gewahrt bleiben. Die Bundesregierung hat diese Grundsätze in mehreren Erklärungen übernommen. Die Realisierung in der Praxis muss jedoch aufmerksam beobachtet werden (Nr. 4.5).

2.1.8 Schulen

Einige wesentliche Punkte aus dem schulischen Bereich:

Das Massaker in Erfurt hat offengelegt, dass Schulen die Eltern volljähriger Schüler ohne deren Einwilligung nicht über wesentliche Ereignisse im schulischen Leben ihres Sohnes oder ihrer Tochter informieren können. In der Beratung einer Änderung des Bayerischen Schulrechts konnte ich erreichen, dass eine gesetzliche Befugnis für derartige Informationen auf bestimmte gravierende Ereignisse beschränkt wird und eine Abwägung mit entgegenstehenden Interessen des Schülers bzw. der Schülerin vorschreibt. Nicht enthalten in der Novellierung ist die ausdrückliche Pflicht, den Schüler oder die Schülerin vor Unterrichtung der Eltern zu informieren. Ich halte das aber für selbstverständlich (Nr. 16.1.1).

Verbrechen in Schulen waren für nicht wenige Schulen auch Anlass, Videoüberwachung zu erwägen. Die Überwachung einzelner Schlüsselbereiche wie der Eingänge halte ich für datenschutzrechtlich möglich, soweit sie aus Sicherheitsgründen für erforderlich gehalten wird, und

Intimbereiche ausgenommen werden. Ich habe aber auch darauf hingewiesen, dass das nicht zur flächendeckenden Dauerüberwachung führen dürfe, und eine Aufsicht durch Personen vorzuziehen ist. Weiter habe ich Beschränkungen hinsichtlich Auswertung und Aufzeichnung – Auswertung nur zur Täterfeststellung oder Beweissicherung, Speicherung maximal für drei Tage – genannt und die Information von Eltern, Lehrern und Schülern, sowie entsprechende Hinweise auf die Videoüberwachung gefordert (Nr. 16.1.4).

In das Lehrer-Fortbildungsprojekt "Intel – Lehren für die Zukunft" konnte ich mich einschalten, nachdem ich von meinem Saarländischen Kollegen auf dieses, von einer Firma initiierte, bundesweite Fortbildungskonzept zur Lehrerweiterbildung hingewiesen wurde. Ich habe veranlasst, dass in die Unterlagen auch datenschutzrechtliche Gesichtspunkte wie Hinweise auf die Risiken des Internets, auf technisch-organisatorische Sicherungsmaßnahmen und auf datenschutzrechtliche Bestimmungen aufgenommen werden. Ich bemängle aber ausdrücklich, dass ich nicht von vorneherein eingeschaltet wurde (Nr. 16.1.3).

2.1.9 Technik und Organisation

Im technisch-organisatorischen Bereich haben mich eine Reihe von Grundsatzthemen beschäftigt, von denen ich exemplarisch einige hier nennen möchte:

Die Entwicklung des Bayerischen Behördennetzes hat u.a. durch die Übertragung der übergreifenden Verantwortung für die Sicherheit auf eine Stelle wesentliche Fortschritte gemacht. Hierdurch wird einer wesentlichen Forderung von mir Rechnung getragen, eine über die Ressortgrenzen hinaus bindende Instanz für die Sicherheit der elektronischen Kommunikation zu schaffen. Andererseits konnte die flächendeckende Umsetzung einer starken Verschlüsselung durch S/MIME-Clients noch nicht erreicht werde. Immerhin sind inzwischen alle Behördenpoststellen mit PGP ausgestattet. Der im Herbst 2002 vollzogene Wechsel des Lizenzinhabers für PGP stellt eine Fortentwicklung des Produktes mit offengelegtem Quellcode und auch die Verfügbarkeit einer Freeware-Version für Privatanwender sicher (Nr. 17.1.1).

Die Projekte zur Einführung von e-government werden weitergeführt. Hervorzuheben ist das Curiavant – Projekt im Raum Nürnberg (früher Media@KOMM), an dessen datenschutzge-

rechter Ausgestaltung ich mitwirke. Ebenso zu nennen ist die Arbeit unter Federführung meine Niedersächsischen Kollegen, mit der ein Kompendium für eine bürgerfreundliche und datenschutzgerechte Ausgestaltung von e-government Anwendungen entwickelt wird. Mit dessen Abschluss rechne ich Anfang 2003 (Nr. 17.1.2).

Ein wichtiges Projekt ist die Entwicklung von Prüfkriterien für datenschutzfreundliche Produkte, sog. Common Criteria. Die im letzten TB angesprochene Entwicklung wurde, zunächst unter meiner Federführung, dann vom Bundesamt für Sicherheit in der Informationstechnik fortgeführt und schließlich mit der Evaluierung und Registrierung zweier Schutzprofile für die „Benutzerbestimmbare Informationsflusskontrolle“ abgeschlossen (Nr. 17.1.3).

Biometrische Verfahren wie die Gesichtsfelderkennung und das Erkennen digitalisierter Fingerabdruck stehen seit dem Terrorismusbekämpfungsgesetz in der öffentlichen Diskussion. Ich habe – auch im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Ländern - dazu vertreten, dass ich zentrale Dateien zur Speicherung biometrischer Daten aller Bürger ablehne. Das gilt insbesondere für die Speicherung von Fingerabdrucken aller Bürger, die damit unverschuldet in polizeiliche Fahndungsmaßnahmen einbezogen werden könnten. Zum Gesamtkomplex nehme ich aus technisch-organisatorischer Sicht unter Nr. 17.1.4. Stellung.

Kostendruck und die immer komplexeren Datenverarbeitungssysteme bringen zunehmend Kommunen zum Outsourcing von DV-Leistungen und zur Auslagerung von Datenbeständen. Ich bin hier vielfach beratend tätig geworden, um mögliche Wege der Realisierung aufzuzeigen, mußte aber auch auf gesetzliche Grenzen und Nachteile hinweisen. In bestimmten Feldern sind dem Outsourcing gesetzliche Grenzen gesetzt, so zum Beispiel in der Verarbeitung von Sozial- oder Meldedaten, in anderen Fällen setzt die Sensibilität der Daten der Auslagerung Grenzen, so z.B. für Patientendaten. Auch die Frage, inwieweit sich die Kommune bei der Erledigung ihrer Aufgaben von privaten Dienstleistern vollständig abhängig machen kann, ist zu überlegen. Im einzelnen verweise ich auf meine Ausführungen unter Nrn. 17.1.5 und 17.3.3.

Im Berichtszeitraum habe ich 10 Einrichtungen auf die Einhaltung der gebotenen technischen und organisatorischen Sicherheitsmaßnahmen geprüft. Das Ergebnis ist unterschiedlich. Män-

gel zeigten sich u.a. in der fehlenden Verschlüsselung bei der Datenübermittlung über das Internet („Sicherheit vergleichbar mit einer offenen Postkarte, die mit Bleistift geschrieben, nicht unterschrieben ist und einem unbekannten auf der Straße zum Transport übergeben wurde“), in der Absicherung gegen Gefahren aus dem Internet (u.a.Viren) und in der Umsetzung der Verpflichtungen aus dem Teledienste- und Medienrecht auf Aufklärung über die Verarbeitung von personenbezogenen Informationen und zur Anbieterkennzeichnung. Diese Verpflichtungen waren vielfach völlig unbekannt.

2.2 Nationale und internationale Zusammenarbeit der Datenschutzbeauftragten

Gerade wegen des grenzüberschreitenden Charakters der Datenverarbeitung muss auch Datenschutz grenzüberschreitend sein. Dazu trägt bei die Europäische Datenschutzrichtlinie EU 95/46/EG mit dem grundsätzlichen Gebot, dass Datenexport in Nicht-EG-Länder ein angemessenes Datenschutzniveau voraussetzt, dazu trägt auch die nationale und internationale Zusammenarbeit der Datenschutzbeauftragten in Datenschutzkonferenzen und ihren Arbeitskreisen bei.

Wie in den vergangenen Jahren habe ich an den halbjährlich Konferenzen der Datenschutzbeauftragten des Bundes und der Länder teilgenommen. Die dort gefassten Beschlüsse, die – nach teilweise ausführlicher Diskussion – sämtliche ohne Gegenstimme, meist einstimmig zustande gekommen sind, sind in der Anlage wiedergegeben. Hervorheben möchte ich hier die Beschlüsse zum "Datenschutz beim elektronischen Geschäftsverkehr" (Anlage 2) aus der 61. Konferenz, zu "Biometrischen Merkmalen in Personalausweisen und Pässen" (Anlage 16), zur Gefährdung von Freiheits- und Persönlichkeitsrechten im Zuge der Terrorismusbekämpfung (Anlage 15) und zu "Datenschutzrechtliche Anforderungen an den Arzneimittelpass" (Anlage 11) aus der 62. Konferenz, sowie "zum Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsanbietern" aus der 63. Konferenz (Anlage 21). Die Verhandlungen der Datenschutzkonferenz werden in Arbeitskreisen vorbereitet, von denen die Federführung für die Arbeitskreise Justiz und Gesundheit und Soziales bei mir liegt.

Auf Internationaler Ebene habe ich bzw. meine Mitarbeiter an den Europäischen Konferenzen in Athen und Bonn sowie an der Internationalen Konferenz in Cardiff im Herbst dieses Jahres teilgenommen. Wesentliche Themen waren Cyberkriminalität und Datenschutz und Arbeitnehmerdatenschutz (Athen), biometrische Identifikationsmerkmale und e-government (Bonn), sowie Videoüberwachung und erneut Biometrie und Telekommunikationsüberwachung (Cardiff)

Nicht zuletzt für eine intensivere Zusammenarbeit und auch Arbeitsteilung unter den Datenschutzbeauftragten beteilige ich mich auch an einem "Virtuellen Datenschutzbüro" (http://www.privacyservice.org/) das auf eine Initiative meines schleswig-holsteinischen Kollegen Helmuth Bäumler zurückgeht. Ich habe das virtuelle Datenschutzbüro in meinem letzten TB ausführlich vorgestellt (19. TB, Nr. 1.1.3). Es soll der Globalisierung und Vernetzung der Datenverarbeitung Rechnung tragen, über das Internet den Bürgern in aller Welt als zentrale Ansprechstelle für jegliche Datenschutzfragen dienen, es soll ein Diskussionsforum für aktuelle Fragen des Datenschutzes bereitstellen, es soll der Datensicherheit sowie der Realisierung von datenschutzfreundlichen Verfahren dienen und nicht zuletzt soll es als eine Plattform für eine weiter verbesserte Zusammenarbeit der Datenschutzbeauftragten fungieren. An dem "Virtuellen Datenschutzbüro" beteiligen sich inzwischen als Projektpartner Datenschutzbeauftragte aus dem In- und Ausland sowohl aus dem staatlichen, wie aus dem Verbands- und Privatbereich.

2.3 In eigener Sache

Zum 31. März dieses Jahres ist meine erste Amtsperiode abgelaufen. Der Bayerische Landtag hat mich auf Vorschlag der Staatsregierung in seiner Sitzung vom 30.01. dieses Jahres mit Wirkung vom 01.04. dieses Jahres mit sehr großer Mehrheit (eine Gegenstimme, sieben Enthaltungen) für eine weitere Amtszeit zum Landesbeauftragten für den Datenschutz gewählt. Über das durch die Wahl ausgesprochene Vertrauen des Bayerischen Landtags habe ich mich sehr gefreut. Ich sehe darin eine Würdigung der Arbeit der Institution Landesbeauftragter für den Datenschutz in Bayern. Wesentlicher Teil dieser Institution ist die Geschäftsstelle des Landesbeauftragten.

Leider hat es inzwischen Entwicklungen gegeben, die bei ihrer vollständigen Realisierung die Arbeitsfähigkeit der Geschäftsstelle wesentlich beeinträchtigt hätten. Der Oberste Rechnungshof hatte in einem Gutachten zur Organisation der Geschäftsstelle vorgeschlagen, die bisherigen vier Verwaltungs- und Rechtsreferate auf zwei Referate, die zwei technisch-organisatorischen Referate auf ein Referat zu kürzen. Mit dieser Verkleinerung sollte eine Herabstufung von drei Referatsleiterstellen verbunden sein.

Angesichts der komplexen Aufgaben meiner Dienststelle, die die Umsetzung der unterschiedlichsten datenschutzrechtlichen Vorschriften in der gesamten öffentlichen Verwaltung in Bayern einschließlich aller Kommunen und Bayerischen Körperschaften und Anstalten beratend begleiten und nachgehend kontrollieren soll, hätte eine derartige Reduzierung der Organisation meiner Dienststelle eine nachhaltige Verschlechterung ihrer Arbeitsfähigkeit und damit eine erhebliche Qualitätsminderung des Produktes "Datenschutz" bedeutet.

Bei der unterschiedlichen Ausgestaltung der datenschutzrechtlichen Vorschriften in den verschiedenen Verwaltungsbereichen – von den Datenschutzvorschriften im Polizeirecht und im Melderecht, über die Datenschutzvorschriften im Sozialbereich bis hin zum Datenschutz im Gesundheitswesen, um nur Beispiele zu nennen – ist auch für den Referatsleiter ein hohes Maß an Spezialwissen zu fordern, das in einem großen Flächenstaat von nur zwei Referatsleitern nicht mehr in der bisherigen Qualität zu gewährleisten wäre.

Die Reduzierung auf zwei Referate im rechtlichen Bereich hätte deswegen eine Verflachung der Arbeit zur Folge gehabt, verbunden mit Flaschenhalssituationen auf der Referatsleiterebene und den damit einhergehenden Verzögerungen.

Realisierbar war dagegen die vom ORH ebenfalls vorgeschlagene Zusammenfassung der zwei technischen Referate.

Inzwischen wurde der Haushalt 2003/2004 meiner Geschäftsstelle im Haushaltsausschuss des Bayerischen Landtags beraten. Die dort beschlossenen Maßgaben erlauben die notwendige Aufrechterhaltung der bisherigen Struktur meiner Geschäftsstelle und die Gleichstellung mit der Ministerialebene, was für die Gewinnung von qualifizierten Mitarbeitern gegenüber den Ministerien von wesentlicher Bedeutung ist.

3 Allgemeines Datenschutzrecht

3.1 Internationales Datenschutzrecht

3.1.1 Inkrafttreten der Europäischen Grundrechtecharta

In der EU-Regierungskonferenz am 07. Dezember 2000 in Nizza wurde die Europäische Charta der Grundrechte von den Staats- und Regierungschefs der Mitgliedsstaaten der EU, dem Präsidenten der Europäischen Kommission und der Präsidentin des Europäischen Parlaments feierlich proklamiert. Die Charta enthält in ihrem Grundrechtekatalog mit Art. 8 auch ein **Grundrecht zum „Schutz personenbezogener Daten“** (vgl. 19. TB, Nr. 2.1.1). Auch wenn die Charta gegenwärtig noch nicht rechtsverbindlich ist, da sie nicht in die Verträge über die Europäische Union aufgenommen wurde, ist diese ausdrückliche Festschreibung des Grundrechts auf Datenschutz ein wichtiger Schritt für die Anerkennung und Verankerung des Datenschutzes in der Europäischen Union. Ich hoffe daher, dass die Grundrechtecharta bald in die Verträge über die Europäische Union aufgenommen werden wird.

3.1.2 Feststellung eines angemessenen Datenschutzniveaus in Drittstaaten

Art. 25 Abs. 1 der EG-Datenschutzrichtlinie schreibt vor, dass eine Übermittlung personenbezogener Daten in ein Drittland, also ein Land außerhalb der EU, grundsätzlich nur zulässig ist, wenn dieses Drittland ein angemessenes Datenschutzniveau gewährleistet. Gemäß Art. 25 Abs. 6 Satz 1 der Richtlinie kann die Kommission - nach Beteiligung des Ausschusses der Regierungsvertreter (Art. 31 der Richtlinie) und Anhörung der Datenschutzgruppe nach Art. 29 - feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Art. 25 Abs. 2 der Richtlinie gewährleistet. Dieses Verfahren hat für bayerische Behörden insofern Bedeutung, als entsprechende Vorschriften zur Zulässigkeit von Datenübermittlungen in Drittländer auch im BayDSG enthalten sind, vgl. Art. 21 Abs. 2 BayDSG.

Mittlerweile gibt es folgende Entscheidungen der Kommission zu dieser Fragestellung:

- Die Kommission hat jeweils mit Entscheidung vom 26. Juli 2000 festgestellt, dass sowohl die **Schweiz** (ABl. L 215/1) als auch **Ungarn** (ABl. L 215/4) ein angemessenes Datenschutzniveau aufweisen.

- Mit Entscheidung vom 20. Dezember 2001 (ABl. L 2/13) stellte die Kommission ferner fest, dass **Kanada** als ein Land angesehen wird, das ein angemessenes Schutzniveau bei der Übermittlung personenbezogener Daten aus der Gemeinschaft an Empfänger garantiert, die der **Personal Information Protection and Electronic Documents Act** unterliegen. Anders als bei der Schweiz und Ungarn bezieht sich die Entscheidung der Kommission also nicht auf Kanada als Drittland, sondern auf dieses Gesetz. Problematisch ist hierbei, dass die übermittelnde Stelle inzident überprüfen muss, ob der potentielle Empfänger diesem kanadischen Gesetz unterfällt. Zum Anwendungsbereich des Gesetzes enthält der Erwägungsgrund 5 der Entscheidung der Kommission nähere Hinweise. Außerdem kann der kanadische Bundesdatenschutzbeauftragte (Federal Privacy Commissioner; www.privcom.gc.ca) zusätzliche Informationen zu derartigen Fällen bereitstellen.

- Das mit den **USA** getroffene Arrangement des „Sicheren Hafens" („Safe Harbor") sieht wiederum einen anderen Ansatzpunkt vor, um ein angemessenes Datenschutzniveau bei der empfangenden Stelle zu gewährleisten. Hierbei führt das US-Handelsministerium ein Verzeichnis von Unternehmen, die sich auf die „Grundsätze des Sicheren Hafens zum Datenschutz" des Handelsministeriums verpflichtet haben. Diese Grundsätze sind in dem Dokument „**Safe Harbor Privacy Principles**" zusammengefasst und werden von 15 „Häufig gestellten Fragen" („FAQ") flankiert. Die Papiere sind auf der Homepage des Bundesbeauftragten für den Datenschutz unter der Adresse www.bfd.bund.de/europa/rubrik3.html abrufbar. Dort befindet sich auch ein Link zur Liste des US-Handelsministeriums mit den Firmen, die sich auf die Grundsätze des sicheren Hafens verpflichtet haben.

3.1.3 Datenschutzvorschriften für die Verwaltungsbehörden der EU

Im Februar 2001 ist die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Daten-

verkehr (ABl. L 008) in Kraft getreten (vgl. 19. TB, Nr. 2.1.2). Die Verordnung enthält Vorschriften, die wie im letzten Tätigkeitsbericht bereits ausgeführt, weitgehend mit den Bestimmungen der EG-Datenschutzrichtlinie übereinstimmen, wie z. B. Zulässigkeitsvoraussetzungen für die Datenverarbeitung, Rechte der Betroffenen bei der Datenverarbeitung, sowie die Bestellung eines obligatorischen Datenschutzbeauftragten für jedes Organ und jede Einrichtung der Gemeinschaft. Als unabhängige Kontrollbehörde wurde ein europäischer Datenschutzbeauftragter eingerichtet, der die Datenschutzrechte im Hinblick auf die Verarbeitung personenbezogener Daten bei Gemeinschaftseinrichtungen sicherzustellen hat.

3.2 Umsetzung der EG-Datenschutzrichtlinie

3.2.1 Novellierung des BDSG

Das novellierte Bundesdatenschutzgesetz (BDSG) ist am 23. Mai 2001 in Kraft getreten (BGBl I S. 904). Dieses Gesetz, das für Bundesbehörden und für die Privatwirtschaft gilt, enthält gegenüber der alten Fassung einige neue und innovative Regelungen, ist jedoch leider recht unübersichtlich und kompliziert geraten. Wichtige (neue) Bestimmungen sind unter anderem (vgl. auch 19. TB, Nr. 2.2.1):

- Eine Regelung zur Datenvermeidung und zur Datensparsamkeit bei der Gestaltung und Auswahl von Datenverarbeitungssystemen, § 3 a BDSG.

- Eine (erweiterte) Vorschrift zur Wirksamkeit der datenschutzrechtlichen Einwilligung, § 4 a BDSG.

- Vorschriften zur Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen, §§ 4 b und 4 c BDSG.

- Eine detaillierte Norm für den Beauftragten für den Datenschutz, den öffentliche und nicht-öffentliche Stellen schriftlich zu bestellen haben, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, § 4 f BDSG. § 4 g BDSG beschreibt dessen Aufgabenbereich näher.

- Eine Regelung zu automatisierten Einzelentscheidungen, § 6 a BDSG.

- Ferner enthält das BDSG nunmehr doch, anders als in dem im letzten Tätigkeitsbericht besprochenen Vorentwurf, eine **Chipkartenregelung**, § 6 c BDSG.

- § 9 a BDSG enthält Regelungen zum Datenschutzaudit.

3.2.2 „Zweite Stufe" der Novellierung des BDSG

Mit der „Ersten Stufe" der Novellierung des BDSG sind Änderungen in Kraft getreten, die über die des novellierten BayDSG hinausgehen. Eine grundlegende Modernisierung des Datenschutzrechts konnte jedoch auch hiermit nicht erreicht werden. Die „Zweite Stufe" der Novellierung des BDSG (vgl. 19. TB, Nr. 2.2.1) steht aus.

Im Zuge der Diskussionen hierzu hat das Bundesministerium des Innern die Professoren Alexander Roßnagel und Andreas Pfitzmann und den Berliner Datenschutzbeauftragten Hans-Jürgen Garstka mit der Erstellung eines Gutachtens zur **„Modernisierung des Datenschutzrechts"** beauftragt. In dessen Entstehung wurden einzelne „Interessensbereiche" mit Hilfe von Workshops einbezogen. Gelegentlich der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder fand am 03. und 04. April 2001 ein Workshop statt, an dem auch ein Vertreter meines Hauses teilgenommen hat.

Das Gutachten ist im Herbst 2001 erschienen und enthält wichtige Anregungen für den „neuen Datenschutz". Es kommt in seinen Thesen unter anderem zu folgenden Ergebnissen, die mir besonders bedenkenswert erscheinen:

- Datenschutz sei **Grundrechtsschutz** (mein langjähriges Motto) und Funktionsbedingung eines demokratischen Gemeinwesens. Daher sollte ein modernes Datenschutzrecht geschaffen werden, das zum einen einfacher und verständlicher und zum anderen angesichts neuer Formen der Datenverarbeitung risikoadäquat sei. Um ersteres Ziel zu erreichen, müsse die Selbstbestimmung der betroffenen Personen gestärkt, sowie die Selbstregulierung und Selbstkontrolle der Datenverarbeiter ermöglicht und verbessert werden. Um das

zweite Ziel zu erreichen, müssten vor allem Konzepte des Selbstdatenschutzes und des Systemdatenschutzes umgesetzt werden.

- Ein modernes Datenschutzrecht sollte auf einem allgemeinen Gesetz gründen, das grundsätzliche und präzise Regelungen zur Datenverarbeitung enthalte und offene Abwägungsklauseln möglichst vermeide. Spezialregelungen in bereichsspezifischen Gesetzen sollten nur Ausnahmen von den allgemeinen Regeln enthalten und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten.

- Die allgemeinen Datenschutzgrundsätze sollten sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich gelten. In beiden Bereichen sei das **gleiche Datenschutzniveau** zu gewährleisten. Unterschiede seien insoweit zu berücksichtigen, als im nicht-öffentlichen Bereich die Regelungsadressaten Grundrechtsträger seien und im öffentlichen Bereich allgemeine Interessen verfolgt werden müssten.

- Jeder Umgang mit personenbezogenen Daten sollte unter der einheitlichen Bezeichnung „Verarbeitung“ subsumiert werden. Dabei sei zwischen der Verarbeitung mit gezieltem Personenbezug und der Verarbeitung ohne gezieltem Personenbezug zu differenzieren, wobei die Anforderungen an letztere risikoadäquat und effizienzsteigernd spezifiziert werden könnten.

- Die Transparenz der Datenverarbeitung gegenüber den betroffenen Personen müsse insbesondere durch ausreichende Informationen erhöht werden.

- Ein genereller Erlaubnistatbestand sollte die Datenverarbeitung immer dann für zulässig erklären, wenn offenkundig keine Beeinträchtigung der betroffenen Personen zu erwarten sei. Soweit Interessen beeinträchtigt werden könnten, sollte die Entscheidung vorrangig der Selbstbestimmung überlassen werden.

- Soweit für die Zwecke der Datenverarbeitung ein Personenbezug nicht erforderlich sei, müsse dieser von Anfang an vermieden oder nachträglich durch Löschung der Daten, ihre Anonymisierung oder Pseudonymisierung beseitigt werden.

- Die Verarbeitung personenbezogener Daten dürfe nur zu bestimmten, in der Einwilligung oder der gesetzlichen Erlaubnis ausdrücklich genannten Zwecken erfolgen (Zweckbindung).

- Datenschutz müsse durch, nicht gegen die Technik erreicht werden. Das Datenschutzrecht müsse datenschutzgerechte Technik fordern und fördern.

- Die Betroffenen müssten ihre Rechte frei und unbehindert sowie unentgeltlich ausüben können.

- Die Datenschutzkontrolle sollte für den öffentlichen und den nicht-öffentlichen Bereich einschließlich der Telekommunikation, der Mediendienste und der Rundfunkanstalten zusammengeführt werden.

Ich hoffe, dass in der „Zweiten Stufe“ eine Novellierung des BDSG diese vielversprechenden Ansätze aufgegriffen werden. Der Wunsch nach einem allgemeinen Gesetz als Schwerpunkt und einer Zurückhaltung bei Sonderregelungen dürfte sich allerdings nur schwer realisieren lassen.

3.2.3 Zuständigkeit des Landesbeauftragten – behördlicher Datenschutzbeauftragter

- Ich halte die Einschätzung des oben angesprochenen Gutachtens zur Modernisierung des Datenschutzrechts, dass die Datenschutzkontrolle soweit wie möglich in einer Stelle zusammengeführt werden sollte, für zutreffend. In meiner täglichen Beratungspraxis habe ich festgestellt, dass nur den wenigsten Petenten - aber auch z. B. Firmen - die Trennung zwischen den Tätigkeitsbereichen des Landesbeauftragten für den Datenschutz und der Aufsichtsbehörde für den nicht-öffentlichen Bereich bekannt ist. Viele Ratsuchende wenden sich wie selbstverständlich an mich. Ferner lassen sich Datenverarbeitungen öffentlicher und nicht-öffentlicher Stellen im zunehmenden Umfang nicht mehr trennen. Häufig arbeiten diese Stellen, wie z. B. Krankenhäuser und niedergelassene Ärzte, private und gesetzliche Krankenversicherungen etc. zusammen. Dies betrifft u.a. telemedizinische Projekte, Ärztenetze und auch Forschungsverbünde. Aber auch die öffentliche Verwaltung bedient sich zunehmend privater Dienstleister soweit das rechtlich zulässig ist (Outsourcing). Auch

hier ist eine datenschutzrechtliche Gesamtkonzeption - ohne Rücksicht auf die Zugehörigkeit der jeweiligen Stelle zu einem bestimmten Bereich - gefragt.

Ich hielte es daher für sachgerecht und zweckmäßig dem Bayerischen Landesbeauftragten für den Datenschutz auch die datenschutzrechtliche Kontrolle **für den nicht-öffentlichen Bereich** zuzuweisen, wie dies bereits in den Stadtstaaten und in den Ländern Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein geschehen ist. In Bayern stehen dieser Lösung seit der letzten Verfassungsänderung allerdings wohl verfassungsrechtliche Bedenken entgegen, da der Landesbeauftragte durch Art. 33 a der Bayerischen Verfassung nicht mehr der Exekutive – der die Datenschutzkontrolle im nicht-öffentlichen Bereich zugehört – sondern dem Bereich des Landtags zugeordnet ist. Eine Zuweisung dieser Aufgaben in meinen Zuständigkeitsbereich würde deshalb wohl eine Verfassungsänderung voraussetzen.

- Das BayDSG schreibt nunmehr die verpflichtende Bestellung interner **Datenschutzbeauftragter** für (fast) alle bayerischen öffentlichen Stellen vor. Im Berichtszeitraum sind daher verstärkt Behörden - aber auch (potentielle) Datenschutzbeauftragte - mit der Frage an mich herangetreten, welche Voraussetzungen ein Datenschutzbeauftragter erfüllen muss.

  Nachstehend stelle ich deshalb zunächst die wesentlichen Neuregelungen dar:

  - Gesetzliche Normierung der Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten (Art. 25 Abs. 2 BayDSG)
    Bisher waren lediglich Sozialversicherungsträger und ihre Verbände gesetzlich (§ 81 Abs. 4 SGB X) zur Bestellung eines behördlichen Datenschutzbeauftragten verpflichtet. Staatliche öffentliche Stellen waren seit 1978 mittels einer Verwaltungsvorschrift (zuletzt Nr. 3.1 der Vollzugsbekanntmachung zum BayDSG vom 05.10.1994) hierzu gehalten und Kommunen war dies aufgrund gleicher Vorschrift nur empfohlen. Nunmehr besteht die Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten für alle öffentlichen Stellen, die personenbezogene Daten mit Hilfe von automatisierten Verfahren bearbeiten.
    Mehrere öffentliche Stellen können auch einen gemeinsamen behördlichen Datenschutzbeauftragten bestellen, wobei dieser allerdings in einer dieser öffentlichen

Stellen beschäftigt sein muss – die Bestellung eines „externen“ Datenschutzbeauftragten, z.B. aus der Privatwirtschaft, scheidet damit aus.

- Gesetzliche Normierung der Stellung eines behördlichen Datenschutzbeauftragten (Art. 25 Abs. 3 BayDSG)
  Durch die Regelungen in den Sätzen 1 mit 5 wird seine Stellung in der öffentlichen Stelle im Vergleich zur bisherigen Situation gestärkt.

- Gesetzliche Normierung der Aufgaben eines behördlichen Datenschutzbeauftragten (Art. 25 Abs. 4 BayDSG)
  Wesentliche Aufgabe des behördlichen Datenschutzbeauftragten ist, auf die Einhaltung des BayDSG und anderer Datenschutzvorschriften in der öffentlichen Stelle hinzuwirken – er ist für deren Einhaltung jedoch nicht verantwortlich. Diese Verantwortung trägt unverändert die speichernde Stelle, d.h. die Leitung der öffentlichen Stelle.
  Andererseits bedeutet diese Aufgabe des behördlichen Datenschutzbeauftragten aber auch, dass er sich zunächst selbst mit der Auslegung und Umsetzung von Datenschutzvorschriften auseinander setzen muss, bevor er sich nach Art. 25 Abs. 3 Satz 3 BayDSG unmittelbar an mich wenden kann und soll. Wendet er sich aufgrund von bestehenden Zweifeln an mich, so sollte er diese Zweifel substantiiert darlegen und soweit möglich auch rechtlich begründen. Leider muss ich aber immer noch und immer wieder feststellen, dass mir von öffentlichen Stellen und von behördlichen Datenschutzbeauftragten Sachverhalte und Vorhaben zur Stellungnahme vorgelegt werden, ohne dass vorher eine angemessene eigene Bewertung durch den behördlichen Datenschutzbeauftragten erfolgt ist. Diese Dienstleistung kann ich aufgrund personeller und zeitlicher Engpässe nicht leisten (siehe hierzu auch Abschnitt 17.2.2, „Erkenntnisse aus Beratungen“).

Die Tätigkeit eines behördlichen Datenschutzbeauftragten ist anspruchsvoll und verlangt ein hohes persönliches und fachliches Engagement. Das BayDSG enthält keine näheren Angaben zu den Anforderungen, die an einen Datenschutzbeauftragten zu stellen sind. § 4 f Abs. 2 Satz 1 BDSG bestimmt dagegen, dass zum Beauftragten für den Datenschutz nur bestellt werden darf, wer die zur Erfüllung seiner Aufgaben erforderliche **Fachkunde** und **Zuverlässigkeit** besitzt. Die Fachkunde umfasst so-

wohl das allgemeine Grundwissen, das jeder Datenschutzbeauftragte aufweisen muss, als auch behörden- bzw. betriebsspezifische Kenntnisse. Zum Grundwissen gehören in erster Linie das Datenschutzrecht, Verständnis für betriebswirtschaftliche Zusammenhänge und Grundkenntnisse über Verfahren und Techniken der automatisierten Datenverarbeitung. Ferner muss der Datenschutzbeauftragte mit der Organisation und den Funktionen seines Betriebs bzw. seiner Behörde vertraut sein.

Vor allem bei der erstmaligen Bestellung zum Datenschutzbeauftragten wird dieses Idealbild nur von wenigen Personen in vollem Umfang erfüllt werden. Daher hat der Dienstherr dem Bestellten auch eine angemessene Einarbeitung und Weiterbildung in diesem Fachgebiet (z. B. durch den Bezug einer Fachzeitschrift, den Erwerb von Fachliteratur und den Besuch von Fortbildungsveranstaltungen) zu ermöglichen.

Zur Zuverlässigkeit eines Datenschutzbeauftragten gehört unter anderem auch, dass diese Tätigkeit nicht mit seinen sonstigen Aufgaben kollidiert. Hierzu und zu seinen Aufgaben habe ich mich in der Orientierungshilfe „Aufgaben eines behördlichen Datenschutzbeauftragten“ geäußert, die auf meiner Homepage (www.datenschutz-bayern.de) in der Rubrik „Technik“ abrufbar ist.

In der Novelle des BayDSG fehlt leider auch eine dem § 4 f Abs. 5 BDSG entsprechende Bestimmung, wonach die öffentlichen (und nichtöffentlichen) Stellen den Beauftragten bei Erfüllung seiner Aufgaben zu unterstützen haben und ihm insbesondere soweit erforderlich Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen haben.

Ich gehe aber davon aus, dass sich diese Verpflichtung auch ohne ausdrückliche Hervorhebung aus der Notwendigkeit ergibt, den behördlichen DSB nicht nur dem Namen nach, sondern effektiv einzurichten.

Im Berichtszeitraum wurde ferner die Frage an mich herangetragen, unter welchen Voraussetzungen die **Abberufung eines Datenschutzbeauftragten** zulässig sei. Ich habe hierzu eine fachliche Stellungnahme des Bayerischen Staatsministeriums des Innern eingeholt, der ich mich inhaltlich anschließe, wobei ich zu dem Ergebnis komme, dass eine Abberufung nur aus wichtigem Grund zulässig ist:

- Die Abberufung eines Datenschutzbeauftragten sei eine Umsetzung oder Teilumsetzung, je nachdem ob es sich um einen vollständigen oder nur teilweisen Aufgabenwechsel handle. Art. 25 Abs. 3 Satz 4 BayDSG untersage eine Benachteiligung des Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben. Aufgabe des Beauftragten sei vor allem, auf die Einhaltung der datenschutzrechtlichen Regelungen hinzuwirken. In der Eigenschaft als Datenschutzbeauftragter bestehe zudem Weisungsfreiheit (Art. 25 Abs. 3 Satz 2 BayDSG). Der für eine (Teil-)Umsetzung erforderliche sachliche Grund könne daher nicht in der ordnungsgemäßen, wenn auch vielleicht aus Sicht eines Behördenleiters zu kritischen Aufgabenerfüllung liegen. Eine offensichtlich **nicht** ordnungsgemäße Aufgabenerfüllung hingegen könne einen sachlichen Grund darstellen.

- Bei der (Teil-)Umsetzung handele es sich nicht um einen Verwaltungsakt. Die **Begründungspflicht** des Art. 39 BayVwVfG finde daher keine Anwendung. Aufgrund des Benachteiligungsverbots sei es jedoch erforderlich, den sachlichen Grund, der der Abberufung als behördlicher Datenschutzbeauftragte zu Grunde liege, anzugeben. Es müsse nämlich gewährleistet sein, dass auch vom Betroffenen selbst nachgeprüft werden könne, ob die Abberufung als behördlicher Datenschutzbeauftragter mit dem gesetzlich verankerten Benachteiligungsverbot vereinbar sei oder nicht.

- Zuständig für die Abberufung sei derjenige, der auch die Bestellungskompetenz inne habe. Bei Staatsbehörden sei dies der jeweilige Behördenleiter. In Kommunen sei für die Bestellung das kommunale Vertretungsorgan zuständig (Gemeinderat, Kreistag, Bezirkstag) oder ein beschließender Ausschuss, dem diese Aufgabe übertragen worden sei. Die Bestellungskompetenz könne durch die Geschäftsordnung auch auf den ersten Bürgermeister, den Landrat oder den Bezirkstagspräsidenten übertragen werden.

- Ein Mitbestimmungsrecht der Personalvertretung bei (Teil-)Umsetzungen bestehe nur dann, wenn sie für die Dauer von mehr als sechs Monaten zur Übertragung von Aufgaben führe, die einem Amt mit höheren oder niedrigerem Endgrundgehalt zugeordnet sind (Art. 75 Abs. 1 Satz 1 Nr. 3 BayPVG) oder mit einem Dienstortwechsel verbunden sind (Art. 75 Abs. 1 Satz 1 Nr. 6 BayPVG). Die Stellung als Datenschutzbeauftragter habe keine besoldungsrechtlichen Auswirkungen. Die Abberufung führe demnach für sich genommen nicht

zu einem Mitbestimmungsrecht der Personalvertretung, soweit sie nicht mit anderen in Art. 75 BayPVG genannten Maßnahmen zusammenträfe.

Besonders wesentlich erscheint mir, dass danach eine Abberufung ohne Begründung unzulässig ist (so auch Kommentar zum BayDSG, Wilde/Ehmann/Niese/Knoblauch, Art. 25 Rdn. 25 a ff.).

Stellung des kommunalen Datenschutzbeauftragten

Die Datenschutzbeauftragte einer bayerischen Kommune fragte bei mir an, ob es rechtens sei, dass sie in ihrer Eigenschaft als kommunale Datenschutzbeauftragte dem Leiter des Hauptamtes unterstellt sei. Ich nahm dazu in Benehmen mit dem Bayerischen Staatsministerium des Innern wie folgt Stellung:

Die behördlichen Datenschutzbeauftragten sind gemäß Art. 25 Abs. 3 BayDSG in dieser Eigenschaft der Leitung der öffentlichen Stelle (Bürgermeister) oder deren ständiger Vertretung unmittelbar zu unterstellen; in Gemeinden können sie auch einem berufsmäßigen Gemeinderatsmitglied (z. B. zweiter Bürgermeister) unterstellt werden. Damit scheidet eine Delegation der Unterstellung auf den Hauptamtsleiter aus, da dieser nicht als ständiger Vertreter im Sinne des Gesetzes anzusehen ist.

4 Gesundheitswesen

4.1 Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Im Februar 2001 ging die Meldung durch die Medien, dass das menschliche Erbgut entschlüsselt worden sei. Der US-Amerikaner Craig Venter und seine Firma Celera Genomics machten geltend, dass ihnen dies als erste gelungen sei. Aber auch das sogenannte Humangenomprojekt (HGP) - ein internationaler Zusammenschluss von Forschern und Forschungsinstituten - beanspruchte die Pionierleistung für sich. Auch wenn die Entschlüsselung der kompletten Sequenz

des menschlichen Genoms nicht mit der Aufdeckung der Wirkungsweise und Funktion aller Gene verwechselt werden darf, ist dies ein großer Schritt in der Erforschung des menschlichen Erbguts. Es ist zu erwarten, dass in den nächsten Jahren und Jahrzehnten große Fortschritte - z. B. bei der Erforschung genetischer Veranlagungen für Krankheiten - gelingen werden. Genetische Informationen, die dem Einzelnen von Anfang an „anhaften“ und ihn individualisierbar machen, besitzen aus datenschutzrechtlicher Sicht jedoch nicht nur in der Forschung große Relevanz. Auch die Bereiche der humangenetischen Beratung und Diagnose (z. B. prädiktive Diagnostik und Vaterschaftstests), der Gentests bei (der Anbahnung von) Beschäftigungsverhältnissen, sowie im Zusammenhang mit Vertragsabschlüssen (z. B. mit Banken und Versicherungen) und der genetischen Analyse zur Strafverfolgung und Prävention besitzen große datenschutzrechtliche Relevanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte deswegen bereits im Oktober 2000 beschlossen, eine Arbeitsgruppe einzusetzen, die sich mit den datenschutzrechtlichen Konsequenzen der Entschlüsselung des menschlichen Genoms beschäftigen sollte. An dieser Arbeitsgruppe unter Leitung des Hamburgischen Datenschutzbeauftragten habe ich teilgenommen. Sie war zunächst mit der Beantwortung eines umfangreichen Fragenkatalogs der durch Beschluss des Deutschen Bundestags eingesetzten Enquete-Kommission „Recht und Ethik der modernen Medizin“ befasst. In der Stellungnahme gegenüber der Kommission wurde die Notwendigkeit einer eigenständigen datenschutzrechtlichen Regelung für den Umgang mit genetischen Daten bejaht. Ein solches Gesetz sei einer standesrechtlichen Regelung über die Satzungsgewalt der Ärztekammern vorzuziehen. Gerade vor dem Hintergrund sich im Ausland abzeichnender Entwicklungen einer Kommerzialisierung von Gendaten erscheine ein formelles „Gendatenschutzgesetz“ geboten.

Eine weitere Aufgabe der Arbeitsgruppe der Datenschutzbeauftragten war es, die datenschutzrechtlichen Anforderungen an die Sicherung der Selbstbestimmung bei genetischen Untersuchungen - evtl. in einem Gesetzentwurf - zu formulieren. In ihrer 62. Sitzung vom 24. bis 26.10.2001 forderten die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung diese Untersuchungen am Menschen gesetzlich zu regeln (vgl. Anlage 12). In einer umfangreichen Anlage wurden Vorschläge für eine solche Regelung gemacht. Geregelt werden sollten demnach die folgenden genetischen Untersuchungen:

- Untersuchungen zu medizinischen Zwecken,

- Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen,
- Untersuchungen zur Abstammungsklärung und Identifizierung außerhalb der Strafverfolgung und
- Untersuchungen zu Forschungszwecken.

Die Datenschutzbeauftragten formulierten ferner wesentliche datenschutzrechtliche Anforderungen an ein solches Gesetz, die durch Ordnungswidrigkeits- und Straftatenbestände abzusichern sind:

- Ein Benachteiligungsverbot bei einer Weigerung, eine genetische Untersuchung durchführen zu lassen,
- die grundsätzliche Erforderlichkeit einer freiwilligen, informierten und schriftlichen Einwilligung des Betroffenen für die Durchführung genetischer Untersuchungen, mit Ausnahme der in einem Gesetz über genetische Untersuchungen zu regelnden und in der StPO geregelten Ausnahmen,
- das Erfordernis einer staatlichen Zulassung für die Durchführung genetischer Untersuchungen zur Gewährleistung der Qualität und Sicherheit dieser Tests,
- ein Arztvorbehalt für das Veranlassen genetischer Untersuchungen,
- eine Zweckbindung bezüglich der erhobenen Daten und Proben,
- Bestimmungen zur Datensicherheit,
- ein unentgeltliches Einsichts- und Auskunftsrecht des Betroffenen,
- eine umfassende Aufklärung und Beratung zur Gewährleistung einer unvoreingenommenen Entscheidung und
- die Festschreibung des Rechts auf Nichtwissen (z. B. bei Forschungsvorhaben).

Ich hoffe, dass es bald zum Erlass eines solchen „Gendatenschutzgesetzes“ kommt, um das informationelle Selbstbestimmungsrecht Betroffener umfassend zu gewährleisten.

4.2 Papier „Einsicht und Information“ des Bremer Diskussionsforums „Charta der Patientenrechte“

Wie ich bereits in meinem 19. Tätigkeitsbericht (Nr. 3.1.1) dargestellt habe, wurde im Jahr 1999 auf der Grundlage eines Gutachtens des Instituts für Gesundheits- und Medizinrecht der Univer-

sität Bremen und auf Initiative der Gesundheitsminister der Länder in Abstimmung mit den wichtigsten organisierten Beteiligten des Gesundheitswesens der Entwurf einer „Charta der Patientenrechte“ vorgestellt. Das hierbei erarbeitete Papier „Gemeinsamer Standpunkt: Patientenrechte in Deutschland heute“ wurde durch die 72. Konferenz der Gesundheitsminister im Juni 1999 verabschiedet.

In der Folgezeit bildete sich an der Universität Bremen ein Diskussionsforum „Charta der Patientenrechte“ zur Umsetzung dieses Papiers. An dem Forum beteiligen sich Akteure des Gesundheitswesens im Lande Bremen wie z. B. der Senator für Gesundheit, die Ärztekammer, die Kassenärztliche Vereinigung, Krankenversicherungen, die Krankenhausgesellschaft, Patientenberatungsstellen und auch der Landesbeauftragte für den Datenschutz. Dieses Diskussionsforum legte im Februar 2001 ein Papier „Einsicht und Information“ vor, dass das Ergebnis eines einjährigen Diskussionsprozesses zu diesen Datenschutzrechten des Patienten darstellt.

Der Arbeitskreis Gesundheit und Soziales der Datenschutzbeauftragten des Bundes und der Länder hat das Papier positiv bewertet. Auf meiner Homepage (www.datenschutz-bayern.de) ist ein Link auf das Papier gesetzt.

Dieses setzt sich insbesondere mit zwei Themenkomplexen auseinander, nämlich den Einsichtsrechten der Patienten in ihre Krankenunterlagen und den Patienteninformationssystemen. Aus datenschutzrechtlicher Sicht ist es hinsichtlich der Einsichtsrechte insofern ein Fortschritt, als es die in der Rechtsprechung vertretene Unterscheidung zwischen objektiven Tatsachen, die der Einsicht unterliegen und subjektiven Bewertungen, die nicht einsichtsfähig sind (vgl. 19. TB Nr. 3.1.1), weitgehend aufgibt und damit für die Betroffenen weitere Einsichtsrechte fordert. Auch die Möglichkeit eine Einsichtnahme aus therapeutischen Gründen zu verweigern, soll begrenzt werden. Als mögliche Gründe für die Verweigerung einer Einsichtnahme werden ausschließlich konkrete Gründe der Selbstgefährdung des Patienten (Gefahr für Leben und Gesundheit) aufgrund der ärztlichen Einschätzung angesehen. Auch bezüglich der Einsichtsrechte in der Psychiatrie und Psychotherapie trifft das Papier umfassende Aussagen, wonach der behandelnde Arzt die Einsichtsgewährung nach folgenden Gesichtspunkten zu entscheiden habe: Die Entscheidung habe sich einerseits an den Persönlichkeitsrechten des Patienten, andererseits an seinem Schutzinteresse (z. B. Möglichkeit einer Selbstgefährdung) zu orientieren.

Ich würde es begrüßen, wenn diese Gedanken Eingang in die oben angesprochene Rechtsprechung und in die einschlägigen Regelungen - z. B. in die Berufsordnung - finden.

Bei den Patienteninformationssystemen wird zwischen „Behandlungsinformationen“ und „Navigatorinformationen“ unterschieden. Erstere sind Informationen, die abstrakt eine Erkrankung und ihre Behandlungsmöglichkeiten beschreiben, letztere sollen dem Patienten die Auswahl der richtigen Behandlung beim richtigen Behandler ermöglichen. Hinsichtlich beider Arten der Information werden in dem Papier Kriterien aufgestellt, die z. B. die Qualität der Information, deren Handhabbarkeit, die Erreichbarkeit und die Kosten betreffen.

4.3 Medizinische Forschungsvorhaben

Auch in diesem Berichtszeitraum hatte ich vielfach Forschungsvorhaben aus dem medizinischen Bereich datenschutzrechtlich zu beurteilen. Exemplarisch will ich nur die beiden folgenden Projekte herausgreifen:

4.3.1 GTH-Hämophilieregister

Die Hämophilie-Kommission der Gesellschaft für Thrombose- und Hämostaseforschung e.V. (GTH) hat sich zum Ziel gesetzt, ein zentrales Register aufzubauen, in dem alle Patienten mit Blutungsneigungen erfasst werden sollen. Das Register ist am Klinikum der Universität München angesiedelt und soll vor allem der Verbesserung der Diagnose und Behandlung von Blutern dienen. Ferner soll eine bessere und engere Kooperation zwischen den Behandlungszentren in Deutschland erreicht und genaue wissenschaftliche Erkenntnisse zu dieser Erkrankung gesammelt werden.

Zunächst war problematisch, dass ich für den GTH e.V., eine nicht-öffentliche Stelle, nicht zuständig bin. Dagegen unterliegt das Klinikum der LMU München meiner Kontrollkompetenz. Gerade in solchen Fällen zeigt sich immer wieder, dass eine Trennung der Kontrollzuständigkeiten zwischen dem öffentlichen und dem nicht-öffentlichen Bereich nicht sinnvoll ist (vgl. Nr. 3.2.3).

Wegen der bundesweiten Bedeutung hat sich auch der Arbeitskreis Gesundheit und Soziales der Datenschutzbeauftragten des Bundes und der Länder mit den Fragen einer datenschutzgerechten Ausgestaltung dieses Vorhabens beschäftigt. So konnten wichtige datenschutzrechtliche Verbesserungen erreicht werden:

- Dem GTH e.V. werden die Daten betroffener Patienten nicht personenbezogen, sondern mittels eines **Pseudonyms** übermittelt. Zur Pseudonymisierung wird der sogenannte RKI-Code verwendet, der sich aus dem dritten Buchstaben des Nachnamens, der Anzahl der Buchstaben des Nachnamens, dem dritten Buchstaben des Vornamens und der Anzahl der Buchstaben des Vornamens zusammensetzt. Ich habe dem GTH e.V. empfohlen, diesen Schlüssel sobald als möglich durch eine Einwegverschlüsselung zu ersetzen, die einen noch höheren Grad an Sicherheit bietet. Diese Empfehlung soll umgesetzt werden, sobald es technisch realisierbar ist.

- Ferner wurden die Einwilligungserklärungen und das Informationsschreiben für die Teilnehmer verbessert, um eine aus datenschutzrechtlicher Sicht notwendige informierte und freiwillige Einwilligung zu gewährleisten. Z. B. wird nunmehr auch ausdrücklich auf die Widerrufsmöglichkeit mit der Folge der Löschung der Daten im Register hingewiesen.

- Außerdem haben sich die Verantwortlichen dahingehend verpflichtet, das Vorhaben mindestens alle zwei Jahre durch den **internen Datenschutzbeauftragten** des Klinikums der TU-München überprüfen zu lassen.

4.3.2 Deutsche Thorotraststudie

Ein weiteres medizinisches Forschungsvorhaben war die Deutsche Thorotraststudie des Deutschen Krebsforschungszentrums (dkfz). Diese Studie ist u.a. auch deshalb von datenschutzrechtlichem Interesse, weil eine Weitergabe von Meldedaten an die wissenschaftliche Einrichtung dkfz beabsichtigt ist und dieses außerdem personenbezogene Auskünfte aus dem vertraulichen Teil der Todesbescheinigung benötigt.

Forschungsinstitute verarbeiten für ihre Forschungsvorhaben oft **Melderegisterdaten**. Häufig handelt es sich bei ihnen - wie beim dkfz - um öffentliche Stellen, so dass sich die Zulässigkeit

der Datenübermittlung nach Art. 31 MeldeG richtet. Gemäß Art. 31 Abs. 1 Satz 1 MeldeG darf die Meldebehörde einer anderen Behörde oder sonstigen öffentlichen Stelle aus dem Melderegister die dort genannten personenbezogenen Daten übermitteln, wenn dies zur Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Bei privaten Forschungseinrichtungen ist die Zulässigkeit von Datenübermittlungen an Art. 34 MeldeG zu messen. In allen Fällen ist jedoch immer zu fragen, ob nicht die Anwendung des Adressmittlungsverfahrens (vgl. 16. TB, Ziff. 8.10) datenschutzgerechter wäre.

Immer wieder stellt sich bei Forschungsvorhaben auch die Frage der Zulässigkeit der Erteilung personenbezogener Auskünfte aus dem vertraulichen Teil der **Todesbescheinigung**. Art. 3 a Abs. 3 Satz 2 Nr. 2 BestG enthält die materiellen Voraussetzungen, unter denen eine solche Auskunft oder Einsicht durch wissenschaftliche Einrichtungen zulässig ist (s. unten). Ob die Voraussetzungen dieser Vorschrift vorliegen, entscheidet die Regierung, in deren Bezirk die Auskunft oder Einsicht gewährt werden soll; betrifft das Forschungsvorhaben mehrere Regierungsbezirke, bestimmt das Staatsministerium für Gesundheit, Ernährung und Verbraucherschutz die zuständige Regierung, vgl. Art. 3 a Abs. 4 Satz 1 BestG i.V.m. Art. 1 Abs. 1 Satz 2 Nr. 14 des Gesetzes über Zuständigkeiten in der Gesundheit, in der Ernährung und im Verbraucherschutz vom 09. April 2001 (GVBl S. 108).

Auskünfte aus dem vertraulichen Teil einer Todesbescheinigung dürfen erteilt oder Einsicht gewährt werden, wenn eine Hochschule oder andere wissenschaftliche Einrichtung die Angaben für ein wissenschaftliches Forschungsvorhaben benötigt und durch sofortige Anonymisierung der Angaben oder auf andere Weise sichergestellt wird, dass schutzwürdige Interessen der verstorbenen Person nicht beeinträchtigt werden, Art. 3 a Abs. 3 Satz 2 Nr. 2 Buchstabe a BestG. Anonymisieren ist gemäß Art. 4 Abs. 8 BayDSG 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 einer bestimmten oder bestimmbaren natürlichen Person (faktische Anonymisierung) zugeordnet werden können. Wird z. B. auf den Todesbescheinigungen nur der Name des Verstorbenen entfernt, sind hierauf unter anderem noch der Wohnort, der Geburtsort, das Geschlecht, der Sterbezeitpunkt, der Sterbeort und das genaue Geburtsdatum enthalten. Diese Angaben - zusammen mit weiteren Angaben - führen dazu, dass die Zuordnung zu einer natürlichen Person nach wie vor möglich ist und eine (faktische) Anonymisierung ausscheidet. Ferner ergibt sich aus dem Begriff der „**sofortigen** Anonymisierung“, dass es nicht ausreicht, wenn die For-

schungseinrichtung die identifizierenden von den sonstigen Daten trennt. Die Trennung muss vielmehr bereits in dem Gesundheitsamt erfolgen, das die Todesbescheinigung aufbewahrt.

Das oben angesprochene Verfahren der Trennung der Daten in der Forschungseinrichtung kann dazu führen, dass „auf andere Weise sichergestellt wird", dass schutzwürdige Interessen des Verstorbenen nicht beeinträchtigt werden. Dabei ist jedoch durch technisch-organisatorische Maßnahmen zuverlässig zu gewährleisten, dass so wenige Personen wie möglich und nur im erforderlichen Umfang die Möglichkeit zur Zusammenführung dieser Daten erhalten. Eine denkbare Lösung wäre auch, einen vertrauenswürdigen Dritten („Treuhänder") zwischenzuschalten, der in genau definierten Fällen die identifizierenden und die sonstigen Daten zusammenführen kann.

Einen Auffangtatbestand enthält Art. 3 a Abs. 3 Satz 2 Nr. 2 Buchstabe b BestG, der Auskünfte und Einsicht auch dann gewährt, wenn das öffentliche Interesse an der Forschung das schutzwürdige Interesse der verstorbenen Person **erheblich** übersteigt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse von Angehörigen der verstorbenen Person an einem Ausschluss der Verarbeitung oder Nutzung überwiegt.

4.4 Inkrafttreten des Infektionsschutzgesetzes

Am 01. Januar 2001 trat des Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten bei Menschen (Infektionsschutzgesetz - IfSG; BGBl I S. 1045 ff.) in Kraft. Gleichzeitig traten das Bundesseuchengesetz und andere Regelungen, wie z. B. das Geschlechtskrankheitengesetz, außer Kraft. Regelungsbereiche, die bisher in mehreren Gesetzen enthalten waren, wurden im IfSG zusammengefasst.

Das IfSG enthält umfangreiche **Meldepflichten**, die unter anderem wegen der medizinischen Fortentwicklung über die bisherigen Meldepflichten des Bundesseuchengesetzes hinausgehen. Hier sind zum großen Teil namentliche, bezüglich bestimmter Krankheiten (z. B. HIV) jedoch auch nicht namentliche Meldungen vorgeschrieben. Bei meldepflichtigen Krankheiten ist die Meldepflicht grundsätzlich von dem feststellenden Arzt und in Krankenhäusern vom leitenden Arzt zu erfüllen. Bei Krankheitserregern trifft diese Pflicht die Leiter von Medizinaluntersu-

chungsämtern und sonstigen privaten oder öffentlichen Untersuchungsstellen einschließlich der Krankenhauslaboratorien. Die nicht-namentliche Meldung erfolgt unter Zuhilfenahme einer fallbezogenen **Verschlüsselung**, die sich aus dem dritten Buchstaben des ersten Vornamens in Verbindung mit der Anzahl der Buchstaben des ersten Vornamens sowie dem dritten Buchstaben des ersten Nachnamens in Verbindung mit der Anzahl der Buchstaben des ersten Nachnamens zusammensetzt, § 10 Abs. 2 IfSG.

Besonderen Augenmerk legt das IfSG auf die **beratende und untersuchende Tätigkeit** der Gesundheitsämter im Bereich sexuell übertragbarer Krankheiten und der Tuberkulose. Gemäß § 19 Abs. 1 Satz 1 IfSG bietet das Gesundheitsamt unter anderem bezüglich sexuell übertragbarer Krankheiten Beratung und Untersuchung an oder stellt diese in Zusammenarbeit mit anderen medizinischen Einrichtungen sicher. § 19 Abs. 1 Satz 2 IfSG bestimmt, dass bei Personen, deren Lebensumstände eine erhöhte Ansteckungsgefahr für sich oder andere mit sich bringen, die Beratung oder Untersuchung auch aufsuchend angeboten werden soll. Die Angebote können bezüglich sexuell übertragbarer Krankheiten **anonym** in Anspruch genommen werden, soweit hierdurch die Geltendmachung von Kostenerstattungsansprüchen nicht gefährdet wird, § 19 Abs. 1 Satz 3 IfSG. Diese rechtlichen Vorgaben des Gesetzes sind von den Gesundheitsämtern zu beachten.

Zu beachten ist ferner, dass im Gegensatz zu § 4 Abs. 1 des Geschlechtskrankheitengesetzes, das am 31. Dezember 2000 außer Kraft getreten ist, das IfSG die Vorlage eines Gesundheitszeugnisses durch Prostituierte nicht mehr vorsieht.

Durch eine Eingabe ist mir in diesem Zusammenhang bekannt geworden, dass das Gesundheitsamt einer Stadt personenbezogene Daten von Prostituierten (aktuelle An- und Abmeldungen, Name, Geburtsdatum und Arbeitsadressen) regelmäßig an die Polizei weitergegeben hat. Ich habe diesen Vorgang wegen Verletzung des Arzt- und Patientengeheimnisses förmlich beanstandet.

Diese Daten wurden im Rahmen der ärztlichen Befundung bei dem Gesundheitsamt erhoben. Die Speicherung der Daten der Prostituierten beruhte nach altem Recht auf § 4 Abs. 1 des Gesetzes zur Bekämpfung von Geschlechtskrankheiten in Verbindung mit Art. 17 Abs. 1 BayDSG. Die Daten unterliegen der ärztlichen Schweigepflicht. Dem steht nicht entgegen, dass keine medizinischen Daten im engeren Sinne an die Polizei weitergegeben wurden, da bereits die Tatsa-

che einer Untersuchung dieser Schweigepflicht unterfällt. Darunter fallen auch Geheimnisse, die bei einer zwangsweisen Untersuchung gewonnen werden. Eine Offenbarungsbefugnis zur zulässigen Durchbrechung der ärztlichen Schweigepflicht lag im vorliegenden Fall nicht vor. Eine solche Befugnis kann sich nicht aus dem allgemeinen Datenschutzrecht - insbesondere dem BayDSG - ergeben, da das BayDSG die Verpflichtung zur Wahrung der in § 203 Abs. 1 StGB genannten Geheimnisse unberührt lässt, Art. 2 Abs. 9 BayDSG. Sonstige Offenbarungsbefugnisse - z. B. aus dem PAG - lagen hier ebenfalls nicht vor.

Diese Praxis ist nach dem Inkrafttreten des IfSG erst recht nicht mehr haltbar, da dieses die Vorlage eines Gesundheitszeugnisses durch Prostituierte überhaupt nicht mehr vorsieht. Für eine regelmäßige Übermittlung der Daten von Prostituierten durch die Gesundheitsabteilungen der Landratsämter an die Polizei ist vor diesem Hintergrund - auch mit Einwilligung der Prostituierten - kein Platz. Da ich im Zuge meiner Überprüfung feststellen konnte, dass auch andere Gesundheitsabteilungen der Landratsämter Vergleichbares praktizieren, habe ich diese angeschrieben und darauf hingewiesen, dass der Schwerpunkt der Tätigkeit der Gesundheitsabteilungen in der gesundheitlichen Aufklärung und Beratung im Sinne des Art. 11 Abs. 1 Satz 2 GDG i.V.m. § 19 Abs. 1 IfSG liege. Eine generelle Aufforderung gegenüber Prostituierten, ihre Einwilligung zu erklären, dass im Zuge der Beratung gewonnene personenbezogene Daten an die Polizei übermittelt werden, ist mit dem vom Gesetzgeber vorgesehenen Beratungsauftrag des Gesundheitsamts unvereinbar.

Davon unberührt bleibt jedoch die in Art. 6 Abs. 2 Satz 2 GDG enthaltene Ausnahme, wonach personenbezogene Daten von den Behörden des öffentlichen Gesundheitsdienstes an öffentliche Stellen übermittelt oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde des öffentlichen Gesundheitsdienstes ist, weitergegeben werden dürfen, wenn dies - im Einzelfall - zur Abwehr von Gefahren für Leben oder Gesundheit Dritter erforderlich ist; der Betroffene soll hierauf hingewiesen werden. Diese Vorschrift kann jedoch nur bezüglich der konkret erforderlichen personenbezogenen Daten derjenigen Prostituierten Anwendung finden, die eine konkrete Gefahr für Leben oder Gesundheit Dritter darstellen. Eine regelmäßige Datenübermittlung kann damit nicht begründet werden. Eine solche Gefahr wäre z. B. dann denkbar, wenn eine Prostituierte an einer ansteckenden Erkrankung leidet und sich nachdrücklich den angeordneten Schutzmaßnahmen (vgl. § 28 IfSG) widersetzt oder der begründete Verdacht besteht, dass sie sich nicht an diese Schutzmaßnahmen halten wird.

Alle angeschriebenen Gesundheitsabteilungen der Landratsämter haben mir die Einstellung dieses Verfahrens bestätigt.

4.5 Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“

Vor dem Hintergrund der „Lipobay-Diskussion“ beschäftigte sich die Öffentlichkeit unter anderem mit der Frage, wie in Zukunft für die Patienten abträgliche Wechselwirkungen verschiedener Medikamente effektiver verhindert werden können. Im Zuge dieser Diskussion wurden aus dem Bundesministerium für Gesundheit Überlegungen zur Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte bekannt, auf der die ärztlichen Verordnungen verzeichnet werden sollen. Zunächst war unklar, ob die Karte für alle (gesetzlich) Versicherten verpflichtend sein solle.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich bereits in den Chipkartenbeschlüssen der 47. und der 50. Datenschutzkonferenz vom 09./10. März 1994 und vom 09./10. November 1995 eingehend mit den datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen beschäftigt. Hiervon ausgehend fassten die Datenschutzbeauftragten in ihrer 62. Datenschutzkonferenz eine Entschließung zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) mit folgenden wesentlichen Inhalten (vgl. Anlage 11):

- Die Datenschutzbeauftragten lehnen eine Medikamentenchipkarte als **Pflichtkarte** ab, da die Patientinnen und Patienten damit unter anderem gezwungen wären, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren.

- Ferner müsse die freie und unbeeinflusste Entscheidung über den Einsatz und die Verwendung der Karte gewährleistet werden.

- Grundlegend sei außerdem die freie Entscheidung der Betroffenen, ob ihre Daten auf einer Chipkarte gespeichert werden, welche Daten auf die Karte aufgenommen und wieder gelöscht werden, ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und wel-

che Daten sie im Einzelfall zugänglich machen (Möglichkeit einer partiellen Freigabe).

- Es wäre datenschutzrechtlich problematisch, den „Arzneimittelpass“ auf der Krankenversichertenkarte gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung der Krankenversichertenkarte wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde.

Im Frühjahr 2002 legte das Bundesministerium für Gesundheit ein Papier **„Eckpunkte zur Einführung der elektronischen Gesundheitskarte“** vor, das datenschutzrechtlichen Vorstellungen weitgehend entgegenkommt. So wird zum Ausdruck gebracht, dass die Gesundheitskarte als freiwilliges Angebot an die Versicherten konzipiert sei. Vor einer flächendeckenden Einführung der Karte sei es erforderlich, sie in Modellprojekten zu erproben. Basis solle die bisherige Krankenversichertenkarte bilden, in der neben der Ausweisfunktion informationstechnisch getrennt ein Arzneimittelpass, Gesundheitsangaben (insbesondere Notfalldaten) und weitere telematische Anwendungen integriert würden. Die Karte solle langfristig auch dazu dienen - unter Anonymisierung oder Pseudonymisierung der Daten - die Generierung dieser Daten zur Qualitätsverbesserung der medizinischen Behandlung zu unterstützen. Das BMG schlägt in dem Papier ferner die Unterteilung der Gesundheitskarte in verschiedene Fächer (z. B. Arzneimittelfach, Notfallinformation, elektronisches Rezept, elektronischer Arztbrief, Verweisfunktion auf Daten, die sich auf Servern befinden etc.) vor.

Ich begrüße es ausdrücklich, dass die Gesundheitskarte in dem Papier als **freiwilliges Angebot** vorgesehen ist. Die Freiwilligkeit der Teilnahme der Patienten muss jedoch nicht nur bei den Modellprojekten, sondern auch später in einer flächendeckenden Umsetzung gewährleistet sein. Bezüglich einer klaren informationstechnischen Trennung der Krankenversichertenkarte von den Funktionen der elektronischen Gesundheitskarte müsste noch ein überzeugendes Konzept vorgelegt werden.

Im übrigen ermöglicht die neue Vorschrift des § 63 Abs. 3 Satz 1 SGB V das Abweichen von den datenschutzrechtlichen Vorschriften im SGB V, soweit dies zur Durchführung (telematischer) **Modellvorhaben** erforderlich ist. Die Datenschutzbeauftragten haben gegen die ursprünglich noch pauschalere Regelung erhebliche datenschutzrechtliche Bedenken vorgetragen und zum Ausdruck gebracht, dass die Vorschriften über das Erheben, Verarbeiten und Nutzen von Sozialdaten nicht alleine durch eine Einwilligung des Versicherten außer Kraft gesetzt wer-

den dürften, sondern im einzelnen geregelt werden müsse, von welchen Vorschriften konkret abgewichen werden könne. Letztlich wurde durch die Intervention der Datenschutzbeauftragten wenigstens erreicht, dass ein Versicherter vor Erteilung der Einwilligung schriftlich darüber zu unterrichten ist, inwieweit ein Modellvorhaben von den datenschutzrechtlichen Vorschriften des SGB V abweicht und aus welchen Gründen diese Abweichungen erforderlich sind. In Bezug auf Modellvorhaben zu **Gesundheitschipkarten** bestimmt das Gesetz nunmehr, dass Erweiterungen der Krankenversichertenkarte nur zulässig sind, wenn die zusätzlichen Daten von den in § 291 Abs. 2 SGB V genannten, ausschließlich administrativen Daten der Krankenversichertenkarte informationstechnisch getrennt werden. Ferner sind Modellvorhaben, in denen von den datenschutzrechtlichen Vorschriften des SGB V abgewichen werden kann, auf längstens fünf Jahre zu befristen und personenbezogene Daten unverzüglich nach Abschluss des Modellvorhabens zu löschen. Der Bundesbeauftragte für den Datenschutz oder die Landesbeauftragten für den Datenschutz sind - jeweils in ihrem Zuständigkeitsbereich - rechtzeitig vor Beginn des Modellvorhabens zu unterrichten. Ich begrüße diese datenschutzrechtlichen Verbesserungen, wenn ich auch für die pauschale Freistellung von den datenschutzrechtlichen Vorschriften in der Modellklausel keinen Grund sehe.

Datenschutzfreundliche Ansätze kommen auch in der **„Gemeinsamen Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“** vom 03. Mai 2002 zum Ausdruck. Die mit dem Ausbau zur Gesundheitskarte verbundene Speicherung und Verarbeitung der Gesundheitsdaten sei als freiwilliges Angebot an die Versicherten zu gestalten. Die Patienten müssten entscheiden können, ob und welche Daten sie einem Leistungserbringer zugänglich machen. Zentral gespeicherte Datensammlungen über Patientinnen und Patienten dürften nicht entstehen. Diese müssten das Recht haben, über sie gespeicherte Daten vollständig zu lesen und die Verwendung gespeicherter Patientendaten dürfe nur innerhalb des gesetzlichen Rahmens unter Wahrung des bestehenden Schutzniveaus (z. B. Beschlagnahmeschutz in der Arztpraxis) erlaubt sein.

4.6 Datenschutzrechtliche Anforderungen an Qualitätssicherungsprojekte

Auch in diesem Berichtszeitraum war ich mehrfach mit der datenschutzrechtlichen Beurteilung von Qualitätssicherungsprojekten (vgl. hierzu auch 19. TB, Ziffer 3.7) befasst. Ich habe die Projektträger darauf hingewiesen, dass bei diesen Qualitätssicherungsprojekten in der Regel **keine**

gesetzlichen Offenbarungsbefugnisse vorliegen, so dass die Verarbeitung personenbezogener Patientendaten - aber auch von Personaldaten - nur mit der freiwilligen, informierten und schriftlichen Einwilligung der Betroffenen zulässig ist. Primär brauchen diese Datenverarbeitungen jedoch nicht personenbezogen, sondern nur anonymisiert (vgl. Art. 4 Abs. 8 BayDSG) erfolgen.

- Die sogenannte Kooperation für Transparenz und Qualität im Krankenhaus (KTQ) trat mit der Bitte um datenschutzrechtliche Hilfestellung an mich heran. Von der KTQ gebildete Teams, die sich aus leitenden Ärzten, Pflegekräften und Verwaltungsdirektoren zusammensetzen, sollen in Krankenhäusern **Visitationen** auf freiwilliger Basis durchführen und diese **zertifizieren**. Es liegt in der Natur der Sache, dass hierbei die Möglichkeit der Kenntnisnahme sensibler Patienten- und Personaldaten durch außenstehende Dritte besteht und solche (unzulässigen) Offenbarungen vermieden werden müssen.

  Zur Vorbereitung der Visitoren auf ihre Tätigkeit hat die Bayerische Landesärztekammer ein Trainingsseminar in München abgehalten, auf dem einer meiner Mitarbeiter einen Vortrag über die Grundlagen des Datenschutzrechts im Allgemeinen und den Datenschutz im medizinischen Bereich im Besonderen gehalten hat.

  Im übrigen habe ich auch an der Erarbeitung eines Datenschutzkapitels für das sogenannte KTQ-Manual für den Einsatz in der Pilotphase mitgewirkt und dabei auch die Einschätzungen des Arbeitskreises Gesundheit und Soziales der Datenschutzbeauftragten des Bundes und der Länder, der sich ebenfalls mit diesem Verfahren beschäftigt hat, eingebracht.

  Ich habe die KTQ unter anderem auf Folgendes hingewiesen:

  - Soweit im Rahmen der Zertifizierung die Verarbeitung von Patientendaten angedacht ist, ist die ärztliche Schweigepflicht zu beachten. Soweit Patientendaten in personenbezogener bzw. personenbeziehbarer Form verarbeitet werden, bedarf es einer Befugnis, um eine zulässige Offenbarung dieser Daten an Dritte - z. B. auch an die Visitoren - annehmen zu können. Nur einige wenige Landeskrankenhausgesetze enthalten Vorschriften, die möglicherweise als Rechtsgrundlage für die Verarbeitung personenbezogener Patientendaten in einem Zertifizierungsverfahren angesehen werden können. Das BayKrG enthält keine solche Bestimmung. Aber auch in den

Ländern, deren Krankenhausgesetze Vorschriften zur Durchführung von Qualitätssicherungsvorhaben enthalten, ist die Verarbeitung personenbezogener Daten nur dann akzeptabel, wenn diese erforderlich ist. Grundsätzlich ist es daher notwendig, die Kenntnisnahme und Verarbeitung personenbezogener Daten durch die Visitoren auf ein Minimum zu beschränken. In den Fällen, in denen es dem Krankenhaus zumutbar ist, die Unterlagen vorher zu anonymisieren oder zu pseudonymisieren, kann auf eine Anonymisierung/Pseudonymisierung nicht verzichtet werden. In Ländern ohne ausdrückliche Rechtsgrundlage ist zu anonymisieren bzw. zu pseudonymisieren, es sei denn, die betroffenen Patienten haben rechtswirksam eingewilligt.

Ich habe die KTQ ferner darauf hingewiesen, dass §§ 137, 113 SGB V auf die freiwillige Zertifizierung von Krankenhäusern keine Anwendung finden. Dies ergibt sich zunächst daraus, dass die Vereinbarungen zur Qualitätssicherung gemäß § 137 Abs. 2 Satz 1 SGB V für zugelassene Krankenhäuser unmittelbar verbindlich sind, während die KTQ eine freiwillige Zertifizierung anbietet. Ferner berechtigt § 137 SGB V externe Prüfer nicht zur Einsichtnahme in Patientenunterlagen. Als datenschutzrechtliche Befugnis zur Einsichtnahme der Prüfer in Daten, die der ärztlichen Schweigepflicht unterliegen, kommt nur § 113 Abs. 2 SGB V in Betracht. Hierzu müssen jedoch die Voraussetzungen gemäß § 113 Abs. 1 Satz 1 SGB V geschaffen werden, wonach die Landesverbände der Krankenkassen, die Verbände der Ersatzkassen und der Landesausschuss des Verbandes der privaten Krankenversicherung gemeinsam die Wirtschaftlichkeit, Leistungsfähigkeit und Qualität der Krankenhausbehandlung eines zugelassenen Krankenhauses durch einvernehmlich mit dem Krankenhausträger bestellte Prüfer untersuchen lassen. Gerade dies ist hier nicht der Fall.

- Ferner habe ich darauf hingewiesen, dass daher in Bayern eine personenbezogene bzw. personenbeziehbare Offenbarung von Patientendaten nur aufgrund der freiwilligen, informierten und schriftlichen **Einwilligung** der Betroffenen zulässig ist. Soweit es von der Organisation der Visitationen möglich ist, die jeweilige Einwilligung des betroffenen Patienten des Krankenhauses zur Einsichtnahme in seine geschützten Daten einzuholen, ist es jedoch datenschutzrechtlich unzulässig, die Behandlung im Krankenhaus von einer solchen Einwilligung abhängig zu machen, da dies mit dem Gebot der Freiwilligkeit im Widerspruch stünde.

- Weiterhin habe ich darauf hingewiesen, dass es vermieden werden sollte, personenbezogene Daten bzw. Unterlagen aus dem Gewahrsam des Krankenhauses zu verbringen, da sonst der **Beschlagnahmeschutz** des § 97 Abs. 2 StPO nicht mehr gegeben ist.

- Ein mit dem Projekt „Freiwillige Krankenhausvergleiche zur externen Qualitätssicherung in der Psychiatrie“ (vgl. 19. TB, Ziffer 3.7.1) vergleichbares Vorhaben ist die „Geriatrie-in-Bayern-Datenbank“ („GiB-DAT-Projekt“) der Arbeitsgemeinschaft zur Förderung der Geriatrie in Bayern (AFGIB). Diese Datenbank soll zur Qualitätssicherung der klinisch geriatrischen Arbeit in Bayern beitragen, indem aus den teilnehmenden Kliniken fortlaufend anonymisierte und standardisierte Informationen über alle Behandlungsfälle erhoben und zentral ausgewertet werden. Hierdurch sollen die teilnehmenden Anstalten die Möglichkeit erhalten, die Ergebnisse der eigenen Arbeit durch den Vergleich mit ähnlichen Einrichtungen besser beurteilen zu können.

  Die Pseudonymisierung der Patientendaten habe ich akzeptiert, da über die klinikinterne Fallnummer nur das Klinikum selbst mit eigenem Zusatzwissen einen Personenbezug herstellen kann. Im übrigen habe ich erreicht, dass z. B. das genaue Geburtsdatum und das genaue Entlassungsdatum, die ein erhebliches Risiko der Identifizierung eines Betroffenen in sich bergen, nicht mehr übermittelt werden.

  In einem sogenannten Follow-Up zum GiB-DAT-Projekt erhalten die Patienten sechs Monate nach der Entlassung aus der geriatrischen Behandlung von der vorbehandelnden Klinik einen Fragebogen mit der Bitte zugeschickt, diesen ausgefüllt wieder an die Klinik zurückzuschicken. Die übermittelten personenbezogenen Daten werden dann entweder von dem Klinikum selbst oder zentral beim GiB-DAT-Projekt in die EDV übertragen.

  Hierzu habe ich darauf hingewiesen, dass bei dem Follow-Up personenbezogene Daten erhoben werden, so dass eine freiwillige, informierte und grundsätzlich schriftliche Einwilligung jedes Betroffenen (Art. 15 Abs. 2 bis 4 BayDSG) erforderlich ist. Ich habe den Projektbetreibern meine Anforderungen an eine freiwillige und informierte Einwilligung (vgl. 19. TB, Ziffer 2.3.1) dargestellt und darauf hingewiesen, dass von der Schriftform der Einwilligung nur abgewichen werden kann, wenn der bestimmte Forschungszweck durch die Schriftform erheblich beeinträchtigt würde, Art. 15 Abs. 3 Satz 2 BayDSG. Die daher

erforderliche schriftliche Einwilligung muss das jeweilige Klinikum für einen angemessenen Zeitraum datenschutzgerecht aufbewahren. Die Fragebögen müssen außerdem datenschutzgerecht vernichtet werden, wenn sie nicht mehr erforderlich seien.

4.7 Datenschutz in den Gesundheitsabteilungen der Landratsämter

Im Berichtszeitraum habe ich - insbesondere ausgehend von meinen Feststellungen im 19. TB (Nr. 3.8) - die Gesundheitsabteilungen sieben bayerischer Landratsämter geprüft. Im Ergebnis konnte ich keine größeren datenschutzrechtlichen Defizite feststellen. Im einzelnen ist mir Folgendes aufgefallen:

- Die **interne Organisation** der Gesundheitsabteilungen der Landratsämter entsprach nicht in allen Fällen dem Mustergeschäftsverteilungsplan für die Landratsämter in der Bekanntmachung des Bayerischen Staatsministeriums des Innern vom 04. Januar 1996 (IZ7-0211.4), da einige Gesundheitsabteilungen nicht in (drei) Sachgebiete entsprechend dieser Vorgaben untergliedert sind.

  In einer Gesundheitsabteilung ist z. B. eine Aufgliederung in Teams erfolgt, die jeweils für bestimmte Gemeinden des Landkreises zuständig sind und weitgehend sowohl Aufgaben aus den Bereichen freiwillige Aufklärung und Beratung als auch hoheitliche Aufgaben wahrnehmen. Zum Teil sind die Gesundheitsämter überhaupt nicht weiter untergliedert. Im wesentlichen wurden die Abweichungen von den Empfehlungen des Bayerischen Staatsministeriums des Innern damit begründet, dass eine weitere Untergliederung einer kleinen Gesundheitsabteilung mit nur wenigen Arztstellen (zwei bis drei) nicht möglich sei. Gerade in Vertretungsfällen lasse sich eine gegenseitige Kenntnisnahme der Vorgänge aus den verschiedenen Bereichen nicht ausschließen. Zum Teil seien die Ärzte auch in verschiedenen Dienststellen im Landkreisgebiet tätig, um eine wohnortnahe Betreuung Hilfesuchender zu gewährleisten.

  Nach wie vor halte ich die Aufteilung der Gesundheitsabteilungen der Landratsämter in drei Sachgebiete mit der Zuweisung der Aufgabenbereiche freiwillige Aufklärung und Beratung an ein Sachgebiet für die beste Lösung, um den gesetzlichen Vorgaben des Art. 6 Abs. 1 Satz 5 GDG gerecht zu werden. Ich habe jedoch Verständnis dafür, dass in relativ

kleinen Gesundheitsabteilungen eine solche Aufteilung sehr schwer durchzuführen und zum Teil sogar unmöglich sein wird. Vor einem solchen Hintergrund halte ich eine abweichende Organisation ausnahmsweise für hinnehmbar. Ich weise jedoch ausdrücklich darauf hin, dass auch in diesen Fällen die Verwertungsverbote des Art. 6 Abs. 1 Satz 1 GDG bezüglich der gesundheitlichen Aufklärung und Beratung, sowie der freiwilligen Untersuchungen und Begutachtungen beachtet werden müssen. Auf Seiten des (ärztlichen) Personals muss gerade hier eine erhebliche Sensibilität für die Wahrung datenschutzrechtlicher Belange an den Tag gelegt werden.

- Auch bei der Ausgestaltung der **Schwangeren(-konflikt)beratung** konnte ich keine wesentlichen Mängel feststellen. Ergänzend zu meinen Ausführungen im 19. TB weise ich noch auf Art. 10 Abs. 1 Satz 3 des Bayerischen Schwangerenberatungsgesetzes (BaySchwBerG) hin, wonach der Name der Schwangeren auf Wunsch nach der Beratung durch eine andere als die beratende Person in die Beratungsbescheinigung eingetragen werden kann. Hierauf sind beratene Frauen zuverlässig hinzuweisen.

- Auch die Führung der **Registratur** und der **Akten** gaben zu keinen Beschwerden Anlass. Die Vorgänge der freiwilligen Untersuchung und Beratung werden zumeist von den Sachbearbeitern selbst - getrennt von den übrigen Aktenbeständen - geführt. Ebenso wenig konnte ich Mängel bei der Führung der **Zentralkartei** feststellen.

- Ferner habe ich bei der Prüfung festgestellt, dass nicht alle Gesundheitsabteilungen über eine **automatisierte Datenverarbeitung** verfügen. In einigen Gesundheitsabteilungen ist diese auch erst im Aufbau begriffen. Einen Anschluss an die Rechner des Landratsamts konnte ich nur bei einem Gesundheitsamt feststellen. In diesem Fall ist das DV-Personal den alleinigen Weisungen des Amtsarztes unterworfen. In den übrigen Fällen, in denen eine ADV verfügbar war, hatten die Gesundheitsabteilungen einen eigenen - von den Rechnern des Landratsamts getrennten - Server (vgl. hierzu 19. TB, Ziffer 17.3.6).

- Hinsichtlich des **Posteinlaufs** habe ich festgestellt, dass schriftliche Maßgaben oder eine Dienstanweisung für die Bediensteten der Poststelle zur Behandlung von Post der Gesundheitsabteilung (z. B. ungeöffnete Weiterleitung von Post an die Schwangerenberatungsstelle und die Aidsberatung) in einigen Fällen fehlten. Ich habe angeregt, dies nachzuholen.

5 Sozialbehörden

5.1 Akteneinsichtsgewährung durch Aktenversand an die Wohnsitzgemeinde

Nach § 25 Abs. 4 Sozialgesetzbuch - SGB - X erfolgt die Akteneinsicht im Sozialverwaltungsverfahren bei der Behörde, die die Akten führt. Im Einzelfall kann die Einsicht aber auch durch eine andere Behörde vermittelt werden. Die Gewährung von Akteneinsicht bei einer wohnortnahen Behörde wie etwa der Wohnsitzgemeinde kann eine willkommene Erleichterung darstellen, vor allem für Bürger mit angegriffenem Gesundheitszustand bzw. Schwerbehinderte. Denkbar ist aber auch, dass dies den Interessen eines Betroffenen zuwider läuft, vor allem wenn die Akte zum Zwecke seiner Einsichtnahme an eine Dienststelle versandt wird, deren Bediensteten er (ohne Zusammenhang mit dem Verwaltungsverfahren) persönlich bekannt ist oder wenn etwa die übersandten Unterlagen auch Angaben über seine Gesundheitsschäden enthalten.

So hatte eine Behörde die Verwaltungsakte mit detaillierten Angaben über die Erkrankung eines Einsichtbegehrenden ausgerechnet der Dienststelle zur Vermittlung der Akteneinsicht übersandt, bei der Betroffene angestellt ist. Der aktenversendenden Dienststelle war diese Konfliktsituation nicht bekannt. Sie glaubte, dem Betroffenen einen Gefallen zu erweisen und hatte ihn nicht vorher informiert, dass sie ihm die beantragte Akteneinsicht bei der Stadtverwaltung seines Wohnsitzes gewähren wolle.

Außerdem hatte die versendende Behörde mit Ausnahme eines schriftlichen Hinweises im Begleitschreiben, dass die Akte Angaben aus dem schutzwürdigen Persönlichkeitsbereich des Betroffenen enthalte und somit Dritten nicht unbefugt zur Kenntnis gelangen dürfe, keine weiteren technischen und organisatorischen Sicherungsmaßnahmen gegen eine unbefugte Einsichtnahme durch Bedienstete der Stadtverwaltung vorgenommen. Der Betroffene beklagte sich bei mir darüber, dass er nun nicht wisse, ob (und falls ja welche) Arbeitskollegen/innen zwischen dem Eingang der Sendung bei der Stadtverwaltung und dem Zeitpunkt seiner Akteneinsicht Details über seinen Gesundheitszustand zur Kenntnis genommen hatten. Einzelne von ihnen, u.a. die mit der Postverteilung Beauftragten, hatten jedenfalls unstreitig Gelegenheit hierzu.

Die aktenversendende Behörde bedauerte diese Misslichkeit sehr und entschuldigte sich beim Betroffenen.

Zur Gewährleistung eines effektiven Schutzes bereits vor dem Risiko einer unbefugten Kenntnisnahme von Sozialdaten durch Bedienstete, denen der Betroffene persönlich bekannt ist, habe ich mit der aktenversendenden Behörde Folgendes vereinbart:

Der Aktenversand zur Einsichtnahme bei einer anderen Behörde wird künftig ausschließlich im Einvernehmen mit der betroffenen Person vorgenommen. Das Einvernehmen des Betroffenen kann auch telefonisch hergestellt werden.

Außerdem wird die Akte in einem (weiteren) verschlossenen Umschlag an die einsichtvermittelnde Behörde verschickt. Der Umschlag mit der Akte erhält einen deutlich erkennbaren Aufkleber mit dem Hinweis, dass er nur durch den vom Akteninhalt betroffenen, namentlich genannten Adressaten der Akteneinsichtsgewährung persönlich geöffnet werden darf. Dieser Hinweis wird im Begleitschreiben wiederholt, das auf den Aktenumschlag geheftet ist bzw. sich zwischen dem ersten und dem zweiten Umschlag des Pakets befindet. Dieses Verfahren ermöglicht, dass das Begleitschreiben zusammen mit der noch eingepackten Akte an die Stelle weitergeleitet werden kann, bei der die Einsichtnahme vermittelt werden soll, etwa beim Bürgerbüro. Die empfangende Behörde wird darüber hinaus im Begleitschreiben aufgefordert, die Akte nach Einsichtnahme durch den Betroffenen noch in dessen Anwesenheit zur Rücksendung zu verpacken.

Durch die Versandart wie bspw. Businesspaket, Einschreiben etc. ist zu gewährleisten, dass anhand des Absendebelegs der aufgebenden Behörde mit der Versandnummer und anhand der Quittung der empfangenden Dienststelle auf entsprechende Nachfrage überprüfbar ist, in welchem Verantwortungbereich sich die Unterlagen gerade befinden.

Ich bitte die Sozialleistungsträger und Sozialversicherungen, die beschriebenen technischen und organisatorischen Sicherungsmaßnahmen zur Gewährleistung des Sozialdatenschutzes beim Aktenversand nach § 25 Abs. 4 SGB X zu übernehmen.

5.2 Ausnahmsweise Übermittlung von Sozialdaten an die Führerscheinstelle zur Überprüfung der Fahrtauglichkeit

Mehrfach wurde die schwierige und umstrittene Frage an mich gerichtet, ob ein Sozialleistungsträger die Führerscheinstelle zur Überprüfung der Fahrtauglichkeit unterrichten darf, wenn ihm bei seiner Aufgabenerfüllung bekannt wird, dass jemand ein Kfz führt, obwohl auf Grund des Gesundheitszustands (z. B. Epilepsie, starker Diabetes) bzw. einer Behinderung schwere Verkehrsgefährdungen zu erwarten sind. Hierzu gilt Folgendes (auch für Sozialversicherungsträger):

§ 69 Sozialgesetzbuch - SGB - X stellt keine Befugnis für die angedachte Sozialdatenübermittlung dar. Insbesondere gehört die erwogene Information der Führerscheinstelle durch den Sozialleistungsträger nicht zu seinen gesetzlichen Aufgaben etwa nach dem BSHG oder nach einem anderen „besonderen Teil“ des SGB i.S.d. § 68 SGB I. Für die reguläre Übermittlung der besagten Sozialdaten an die Führerscheinstelle gibt es auch keine sonstige gesetzliche Befugnis im SGB. Nach § 67 d Abs. 1 SGB X ist eine Übermittlung von Sozialdaten aber nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im SGB einschlägig ist.

Für seltene und besonders gelagerte Ausnahmen, in denen sich dem Sozialleistungsträger nach sorgfältiger Einschätzung des jeweiligen Einzelfalles aufdrängt, dass sich aus einer Krankheit oder einem Gebrechen des betroffenen Antragstellers bzw. Leistungsbeziehers konkrete Gefahren für Leib und Leben Dritter ergeben, wird in der Literatur allerdings nicht ausgeschlossen, dass die Übermittlung der zur Gefahrenabwendung erforderlichen Sozialdaten unter Berufung auf einen rechtfertigenden Notstand nach § 34 Strafgesetzbuch (StGB) vertretbar sein kann. Ein anderer Teil der Literatur begründet die ausnahmsweise Vertretbarkeit der Datenübermittlung verfassungsrechtlich mit der aus Art. 2 Abs. 2 S. 1 i.V.m. Art. 1 Abs. 1 S. 2 des Grundgesetzes abgeleiteten Pflicht des Staates, das menschliche Leben umfassend zu schützen und es vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren. Insoweit bestehe in extremen Ausnahmefällen nach dem Prinzip der Einheit der Rechtsordnung ein rechtfertigender Notstand auch für Staatsorgane.

Für die genannten seltenen und besonders gelagerten Ausnahmefälle möchte ich mich den besagten Datenübermittlungen im Hinblick auf die hohe Schutzbedürftigkeit von Leben und Ge-

sundheit und unter Bezugnahme auf die o.g. Meinungen in der Literatur nicht verschließen, vorausgesetzt sie erfolgen nach Prüfung folgender Voraussetzungen bzw. unter Einhaltung folgender Maßnahmen:

Weil der rechtfertigende Notstand voraussetzt, dass sich aus der gesundheitlichen Beeinträchtigung und der daraus - nach dem insbesondere anhand vorliegender ärztlicher Informationen abzusichernden Erkenntnisstand des Sozialleistungsträgers - resultierenden Fahruntauglichkeit eine **gegenwärtige, nicht anders abwendbare Gefahr** für Leben bzw. Gesundheit Dritter ergibt, hat der Sozialleistungsträger bei Bejahen der Fahruntauglichkeit durch Nachfrage beim Betroffenen zu klären, ob dieser im Besitz eines Führerscheins ist und ob sich aktuell überhaupt Gelegenheiten bieten, ein Kfz zu führen. Vielfach dürfte sich schon im Zuge dieser Überprüfungen zeigen, dass die o.g. Gefahrenlage i.S.d. § 34 StGB nicht gegeben ist. Andernfalls muss eingeschätzt werden, ob der Betroffene einsichtig und verlässlich genug ist, für die Dauer seiner einschlägigen Erkrankung vom Führen eines Kfz abzusehen.

Steht dies nicht zu erwarten, muss nunmehr versucht werden, seine Einwilligung in die Information der Führerscheinstelle zu erhalten, selbst wenn diese Zustimmung unwahrscheinlich sein mag. Die Berufung auf einen rechtfertigenden Notstand i.S.d. § 34 StGB als „ultima ratio“ zur Rechtfertigung einer vom SGB regulär nicht zugelassenen Datenübermittlung setzt nämlich voraus, dass diese Information nicht auf die Einwilligung des Betroffenen gestützt werden kann, weil in diesem Falle kein belastender Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen erforderlich wäre.

Die beschriebene Vorgehensweise des Sozialleistungsträgers ist außer zur Feststellung der Gefahrenlage auch deshalb notwendig, um Informationsgrundlagen für die unverzichtbare Abwägung der widerstreitenden Interessen i.S.d. § 34 StGB zu gewinnen. Des Weiteren muss die Information der Führerscheinstelle ein angemessenes Mittel sein, die Gefahr für die genannten Rechtsgüter Dritter abzuwenden (vgl. § 34 S. 2 StGB).

Die Prüfung und Entscheidung, ob die Führerscheinstelle ausnahmsweise informiert werden darf, sollte unbedingt einer Person mit Vorgesetztenfunktion übertragen werden, etwa dem Leiter des Sozialleistungsträgers oder seinem Stellvertreter.

Nur unter den genannten Voraussetzungen und nur bei äußerst restriktiver und sorgfältiger Fallselektion kommt die Information der Führerscheinstelle über die gesundheitsbedingte Untauglichkeit eines Betroffenen zum Führen eines Kfz als vertretbar in Betracht. Obwohl die gesundheitlichen Angaben dem Sozialleistungsträger womöglich von einem Arzt zugänglich gemacht wurden, steht § 76 SGB X der Informationsweitergabe nicht entgegen. Auch der Arzt wäre nämlich unter den Voraussetzungen des rechtfertigenden Notstands nach § 34 StGB im extremen Ausnahmefall zur Offenbarung dieser gesundheitlichen Defizite gegenüber der Führerscheinstelle berechtigt.

5.3 Gesetzliche Krankenversicherung

5.3.1 Strukturierte Behandlungsprogramme bei chronischen Krankheiten (Disease-Management-Programme / DMPe) nach dem Gesetz zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung

Im o.g. Risikostrukturausgleichsgesetz vom 10.12.2001 hat der Gesetzgeber beim Risikostrukturausgleich zwischen den Krankenkassen die besondere Berücksichtigung von Ausgaben für chronisch kranke Versicherte vorgesehen, wenn sie in „zugelassene strukturierte Behandlungsprogramme (DMPe)“ eingeschrieben sind. Als DMP wird eine medizinische Versorgungsform bezeichnet, mit der der Behandlungsablauf und die Qualität der medizinischen Versorgung chronisch Kranker optimiert werden sollen. Disease-Management in diesem Sinne setzt regelmäßig verbindliche und aufeinander abgestimmte Behandlungsprozesse voraus, die auf der Grundlage medizinischer Evidenz festgelegt werden. Vorerst wurden Brustkrebs- und Diabetes-mellitus-Erkrankungen als für die Entwicklung von DMPen geeignete chronische Krankheiten festgelegt. Geplant sind außerdem Behandlungsleitlinien für chronische Atemwegserkrankungen wie Asthma und für koronare Herzerkrankungen.

Für die Krankenversicherten ist die Teilnahme an einem von der Krankenkasse angebotenen zugelassenen DMP freiwillig, sie setzt zusätzlich nach § 137 f Abs. 3 Sozialgesetzbuch - SGB - V die Einwilligung zur Erhebung, Verarbeitung und Nutzung der in der Risikostrukturausgleichsverordnung zum jeweiligen DMP festgelegten Daten seitens der Krankenkasse und zur Übermittlung dieser Daten an die Krankenkasse voraus.

Trotz dieser Einwilligung ist die Übermittlung der Angaben aus der ärztlichen Behandlung, die vom Bundesministerium für Gesundheit (BMG) durch Verordnung festgelegt wurden, datenschutzrechtlich problematisch. Es widerspricht nämlich grundsätzlich den datenschutzrechtlichen Zielvorstellungen, dass die Krankenkassen versichertenbezogen und fortlaufend detaillierte Dokumentationen mit Angaben über ärztliche Behandlungen und den Krankheitszustand einschließlich Befunden und Laborparametern erhalten. Des Weiteren haben die Kassenärztlichen Vereinigungen (KVen) aufgrund einer Sonderregelung in § 295 Abs. 2 S. 4 SGB V bei der Teilnahme des Versicherten an einem DMP die Abrechnungsdaten mit Benennung der erbrachten vertragsärztlichen Leistungen - abweichend von der sonstigen vertragsärztlichen Versorgung - versichertenbezogen an die Krankenkasse zu übermitteln.

Gegen diese Entwicklung haben die Datenschutzbeauftragten Einwände erhoben, sowohl während des Gesetzgebungsverfahrens zum Risikostrukturausgleichsgesetz als auch im Verfahren der Verordnungsgebung des BMG, in dem u.a. die Anforderungen an die Inhalte der an die Krankenkassen gehenden ärztlichen Dokumentationen in der Risikostrukturausgleichsverordnung (RSAV) rechtsverbindlich festgelegt wurden. Wir haben darauf hingewiesen, dass der Umfang, in dem die Krankenkasse Patienten- und Leistungsdaten aus der DMP-Behandlung versichertenbezogen benötigt, davon abhängt, welche Rolle den Krankenkassen hinsichtlich der DMPe zukommt.

Die Krankenkassen berufen sich mit Unterstützung des BMG darauf, dass der Gesetzgeber die Durchführung von DMPen ihnen übertragen habe. Aufgrund der Datenerhebungs- und -verwendungsbefugnis in § 284 Abs. 1 S. 1 Nr. 11 SGB V u.a. zur „Vorbereitung und Durchführung“ der DMPe und der Verpflichtung der Landes- und Spitzenverbände der Krankenkassen durch § 137 f Abs. 5 SGB V, ihre Mitgliedskassen bei dem „Aufbau und der Durchführung von strukturierten Behandlungsprogrammen“ zu unterstützen, ist die Plausibilität einer solch grundsätzlichen Aufgabenzuweisung an die Krankenkasse, auch im Hinblick auf die Auswirkungen der DMPe auf den Risikostrukturausgleich, nicht von der Hand zu weisen. Ich hätte mir in Anbetracht der tiefgreifenden Eingriffe in die Persönlichkeitssphäre der Patienten durch die Datenübermittlungen jedoch eine ausdrückliche Festlegung im Gesetz gewünscht, welche konkreten Aufgaben die Krankenkassen bei der Durchführung der DMPe zu übernehmen haben.

Nach § 137 f Abs. 5 SGB V sind die Krankenkassen berechtigt, wenn auch nicht verpflichtet, ihre Aufgaben zur Durchführung von DMPen auf Dritte zu übertragen. Aufgrund dessen habe

ich mich für die Aufnahme einer Öffnungsklausel in die RSAV eingesetzt, wonach im Falle und nach Maßgabe entsprechender vertraglicher Vereinbarungen der Krankenkasse mit den ärztlichen Leistungserbringern die Übermittlung pseudonymisierter Dokumentationen an die Krankenkasse ausreichen soll. Das BMG als Verordnungsgeber der RSAV ist dieser Anregung teilweise nachgekommen:

Beim Zustandekommen von Vereinbarungen zwischen Krankenkassen und Ärzten über die DMP-Durchführung nach § 28 f Abs. 2 RSAV muss der Krankenkasse lediglich eine inhaltlich reduzierte Fassung der ärztlichen Dokumentation versichertenbezogen übermittelt werden. Die Inhalte der ausführlichen ärztlichen Dokumentation werden von einer Arbeitsgemeinschaft der Krankenkassen und Kassenärztlichen Vereinigungen pseudonymisiert und an eine von den Mitgliedern der Arbeitsgemeinschaft gebildete gemeinsame Einrichtung zur Qualitätssicherung übermittelt. Die Krankenkasse darf die Wiederherstellung des Versichertenbezugs von der Arbeitsgemeinschaft nur verlangen, wenn dies im Einzelfall für die Erfüllung der jeweiligen Aufgabe zur Qualitätsprüfung oder zur Sicherstellung der Vollständigkeit und Plausibilität der erstellten ärztlichen Dokumentationen, also ausnahmsweise, erforderlich ist.

Des Weiteren entsprach das BMG den Forderungen der Datenschutzbeauftragten, dass die vom Arzt zu übermittelnden DMP-Dokumentationen nur die in der RSAV jeweils aufgeführten Angaben umfassen und nur für Zwecke der DMP-Durchführung verwendet werden dürfen. Zugang zu den DMP-Dokumentationen dürfen bei den Krankenkassen außerdem nur Personen haben, die Aufgaben im Rahmen der Betreuung Versicherter in strukturierten Behandlungsprogrammen wahrnehmen und hierfür besonders geschult worden sind. Ebenso verlangt die RSAV in Ergänzung des § 137 f Abs. 3 SGB V ausführliche Informationen der DMP-Teilnehmer zu den Programminhalten und zu den Datenübermittlungen an und Datenverwendungen durch die Krankenkasse („informierte Einwilligung“). Einwilligen muss der Versicherte nach der RSAV auch in jede einzelne Übermittlung seiner Gesundheitsdaten vom Arzt an die Krankenkasse, so dass er von seinem Arzt aktuell darüber informiert wird, welche Patientendaten dieser unmittelbar an die Krankenkasse weitergibt.

5.3.2 Entwurf eines Transparenzgesetzes und Verbesserung der Datentransparenz in der gesetzlichen Krankenversicherung durch einen Datenpool

In meinem 19. Tätigkeitsbericht habe ich unter Ziffer 4.2.1 über die ursprünglich im Gesetzgebungsvorhaben zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 mit enthaltenen datenschutzrechtlichen Änderungen berichtet und ebenso, dass dieser Gesetzentwurf zwar vom Bundestag beschlossen, dann aber wegen andersgearteter gesundheitspolitischer Erwägungen vom Bundesrat abgelehnt worden war. Mit diesen Fragen muss ich mich als Leiter des Arbeitkreises „Gesundheit und Soziales“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder besonders befassen.

Das Bundesministerium für Gesundheit (BMG) hat daraufhin Anfang 2001 einen Arbeitsentwurf zu einem „Gesetz zur Verbesserung der Datentransparenz und des Datenschutzes in der gesetzlichen Krankenversicherung (Transparenzgesetz - GKV-TG)“ zur datenschutzrechtlichen Erörterung übersandt, diesen Gesetzentwurf dann aber wegen des Widerstands der Krankenkassen gegen einzelne Pseudonymisierungsregelungen nicht mehr weiter verfolgt.

Weiter entwickeln möchte das BMG aber seine bereits aus den genannten bisherigen Gesetzesvorbereitungen ersichtlichen Vorhaben einer Verbesserung der Datentransparenz und der Datengrundlagen zur Steuerung des Leistungs- und Ausgabengeschehens der gesetzlichen Krankenversicherung und für die Gesundheitsberichterstattung des Bundes und der Länder. Notwendig ist hierzu eine verbesserte Bereitstellung steuerungsrelevanter Daten durch eine kassenartenübergreifende Datenzusammenführung in einem **Datenpool für Steuerungsaufgaben der gesetzlichen Krankenversicherung**. Dieser soll eine valide Datenbasis sein u.a. für die Analyse von Behandlungsabläufen (u.a. bei chronisch Kranken) zur Verbesserung der Wirtschaftlichkeit und Qualität, für eine Auswertung des Versorgungsgeschehens als Grundlage von Planungen und Maßnahmen (bspw. zur Korrektur einer regionalen Über-, Unter- und Fehlversorgung) und für eine Unterstützung politischer Entscheidungsprozesse zur Weiterentwicklung der GKV (Gesundheits- und Versorgungsziele).

Nach der übereinstimmenden Auffassung aller beteiligten Diskussionspartner, nämlich der Krankenkassen, der ärztlichen Leistungserbringer, des BMG und der Vertreter aus der Politik

sowie der Datenschutzbeauftragten von Bund und Ländern, werden für diese Ziele keine personenbezogenen Daten benötigt. Einen Pool mit konkret personenbezogenen Patientendaten hätte ich wegen der damit verbundenen Entwicklung hin zum gläsernen Patienten entschieden abgelehnt. Eine Anonymisierung der Daten im Datenpool ist allerdings insoweit nicht möglich als neu hinzukommende Daten den bereits zum jeweiligen Individuum gespeicherten Daten zugeordnet werden müssen. Die Notwendigkeit eines Datenpools für die o.g. Zielsetzungen mit pseudonymisierten Daten, d.h. mit Daten, die sich nur auf einen Fall, nicht aber auf eine konkrete Person beziehen, erachte ich als plausibel. Ich erkenne an, dass die derzeitige Aufsplitterung der Abrechnungen auf verschiedene Leistungssektoren und auf eine Vielzahl von Krankenkassen und Kassenärztliche Vereinigungen eine valide Datenbasis für behandlungssektoren- und kassenartenübergreifende Auswertungen bisher verhindert. Ich frage aber, ob für diese Zwecke nicht auch eine genügend große Stichprobenerhebung ausreicht. Der Leiter der zuständigen Abteilung im BMG hat dazu auf dem 11. Wiesbadener Datenschutzforum am 19.09.2002 erklärt, dass diese Frage noch nicht entschieden sei. Die vorstehend genannte Pseudonymisierung muss gewährleisten, dass ein Rückschluss auf die konkrete Person zuverlässig ausgeschlossen ist.

Die Datenschutzbeauftragten des Bundes und der Länder haben dem BMG ihre datenschutzrechtlichen Anforderungen an die Datenzusammenführung in einem Datenpool in der GKV mitgeteilt. Die wichtigsten Forderungen sind:

- Die einzelnen Zwecke der Datenaufbereitung und die Zugriffsberechtigungen sind gesetzlich abschließend zu regeln. Es darf nicht zunächst der Datenpool geschaffen und dann erst überlegt werden, was man damit alles machen kann.
- Die Daten sowohl der Versicherten als auch der Leistungserbringer sind zu pseudonymisieren. Reidentifikationen sind zu unterbinden.
- Das absolute Reidentifikationsverbot muss technisch durch ein sicheres Pseudonymisierungsverfahren, faktisch durch den Umfang der Datenübermittlungen und rechtlich durch entsprechende gesetzliche Regelungen abgesichert werden.
- Nur aggregierte Auswertungen dürfen gesetzlich zugelassen werden.
- Die Vertrauensstelle, in der die Pseudonymisierung durchgeführt wird, und die Datenaufbereitungsstelle - der eigentliche „Datenpool“ - sind in öffentlich-rechtlicher Rechtsform und als Stellen, die das Sozialgeheimnis nach § 35 Abs. 1 SGB I zu wahren haben, zu konzipieren.

- Diese Stellen sind räumlich, organisatorisch und personell von den Krankenkassen und deren Verbänden, den Kassenärztlichen Vereinigungen und sonstigen abrufberechtigten Stellen zu trennen.

5.3.3 Einholen von Gegen-Kostenvoranschlägen durch Krankenkassen bei weiteren Hilfsmittelerbringern

Aus Gründen des Wirtschaftlichkeitsgebots nach den §§ 2, 12 und 127 Abs. 3 Sozialgesetzbuch - SGB - V sind die Krankenkassen gehalten, bei nicht standardisierten Versorgungen mit Hilfsmitteln wie etwa Prothesen und orthopädischen Schuhen Vergleichsangebote, sog. „Gegen-Kostenvoranschläge“ einzuholen. Eine Befugnis zur Übermittlung personenbezogener Versichertendaten (Sozialdaten) ist damit aber noch nicht verbunden.

Diese Befugnis würde sich aus § 284 Abs. 1 S. 1 Nr. 4 i.V.m. Abs. 3 SGB V ergeben, soweit diese Daten u.a. für die Gewährung von Leistungen an Versicherte erforderlich sind. Diese Notwendigkeit ist nicht gegeben, wenn der weitere Kostenvoranschlag anhand einer von der Krankenkasse pseudonymisierten Kopie der Verordnung in Auftrag gegeben werden kann. Die Krankenkasse hat dann den Versichertenbezug, nicht aber der weitere Hilfsmittelerbringer, an den sich der Versicherte nicht gewandt hat.

Selbst in den Fällen, in denen Hilfsmittel später körper- bzw. behindertengerecht angefertigt werden müssen, wie etwa bei orthopädischen Schuhen und Beinprothesen, muss der Versicherte dem weiteren Hilfsmittelerbringer gegenüber vielfach nicht benannt werden, nämlich dann nicht, wenn dieser den Kostenvoranschlag allein aufgrund von Maßangaben erstellen kann. Nur wenn sich bereits der Kostenvoranschlag für eine Spezialanfertigung nicht ohne persönliches Maßnehmen bzw. nicht ohne persönliche Kontaktaufnahme dieses Hilfsmittelerbringers mit dem Betroffenen erstellen lässt, kommt hierfür die Mitteilung der Identität des Versicherten in Betracht. Solche Fälle und die übermittelten personenbezogenen Daten sind für Prüf- und Auskunftszwecke zu dokumentieren. In diesen Fällen ist auch eine Benachrichtigung des Versicherten notwendig.

5.4 Kassenärztliche Vereinigung Bayerns (KVB)

5.4.1 Laborüberweisungen ohne Identitäten der Patienten

In den letzten Jahren ist ein zunehmender Konzentrationsprozess medizinischer Patientendaten im Bereich fachärztlicher Laboratorien zu beobachten. Wie mir berichtet wurde, sind Laboratorien mit jährlich 400.000 Fällen keine Seltenheit mehr; die größten Labors würden pro Jahr sogar 2 bis 4 Millionen Fälle abrechnen. Mit dem Untersuchungsauftrag an das Labor werden die genaue Diagnose oder Verdachtsdiagnose und wichtige Befunde angegeben. Nach erfolgter Untersuchung werden diese Daten im Labor mit den Ergebnissen zusammengeführt und gespeichert. Technisch dürfte es kein Problem sein, die Patientendaten z.B. nach Krankheitsbildern auszuwerten. Aus Datenschutzsicht handelt es sich angesichts dieser Mengen von Patientendaten in privaten Datenbanken um eine im Hinblick auf das Recht auf informationelle Selbstbestimmung der Betroffenen durchaus bedenkliche Entwicklung.

Ich habe die KVB daher um Stellungnahme gebeten, ob Laboraufträge dadurch datenschutzfreundlicher gestaltet werden können, dass sie hinsichtlich der Patientenidentitäten regelmäßig nur noch pseudonymisiert, bspw. durch Verwendung von Codes, erteilt werden.

Die Frage, ob eine Codierung bei Laboraufträgen nicht eine bedenklich erhöhte Verwechslungsgefahr bei der Zuordnung von Untersuchungsergebnissen zum betreffenden Patienten zur Folge hat, wird unterschiedlich beurteilt. Ich gehe davon aus, dass die Sicherheit vor Verwechslungen der Laborproben eine Frage der technischen Ausgestaltung und der Zuverlässigkeit des Codierungsverfahrens ist. Auch staatliche Gesundheitsämter beauftragen private Labors mit codierten/pseudonymisierten Unterlagen und Materialien, z.B. in Baden-Württemberg. Selbst wenn für einzelne noch zu definierende Ausnahmen, wie etwa bei labormeldepflichtigen Infektionen, auf den Patientenbezug nicht verzichtet werden könnte, würde das regelmäßige Absehen von der Mitteilung der Identität des jeweiligen Patienten bzw. Versicherten an das Labor dennoch einen großen Fortschritt gegenüber der derzeitigen Praxis darstellen.

Im Einvernehmen mit meinen Datenschutzkollegen habe ich mich an den Bundesbeauftragten für den Datenschutz (BfD) gewandt, damit er Verhandlungen mit der Kassenärztlichen Bundesvereinigung (KBV) und der Bundesärztekammer (BÄK) mit dem Ziel aufnimmt, dass Laborüberweisungen ohne Offenlegung der Identitäten der jeweiligen Versicherten erfolgen. Das La-

bor benötigt nämlich selbst für Laborleistungen, die es mit der Krankenkasse abzurechnen hat, lediglich die Kenntnis der Krankenversichertennummer und der Krankenkasse des Versicherten. Aus medizinischen Gründen dürfte es regelmäßig erforderlich sein, dem Laborarzt zusätzlich noch das Geschlecht und das Geburtsjahr des Patienten mitzuteilen. Die Umstellung auf dieses Verfahren wäre ohne größeren Aufwand möglich und die vertraglich festgelegten Abrechnungswege könnten bestehen bleiben.

Die Korrespondenz des BfD mit der KBV und der BÄK dauert noch an.

5.4.2 Korrektur einer Auskunft nach § 305 SGB V über die bei der Kassenärztlichen Vereinigung Bayerns (KVB) gespeicherten vertragsärztlichen Abrechnungsdaten

Nach § 305 Abs. 1 S. 1 und 2 Sozialgesetzbuch - SGB - V sind die Kassenärztlichen Vereinigungen (KVen) und die Krankenkassen verpflichtet, die Versicherten auf deren Antrag über die im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und deren Kosten zu unterrichten. Die KVen haben den Krankenkassen hierzu die entsprechenden Angaben über die vertragsärztlichen Leistungen und deren Kosten in einem weiteren verschlossenen Umschlag zur Weiterleitung an den Auskunftsuchenden zu übermitteln. Die Krankenkasse fügt ihre Auskunftsbestandteile hinzu und übersendet das Gesamtergebnis an den Auskunftsuchenden, ohne den Inhalt der seitens der KV erteilten Auskunft zu kennen.

Aufgrund einer solchen Versichertenauskunft hatte ein Patient festgestellt, dass sein behandelnder Arzt mit der KVB Leistungen abgerechnet hatte, die er nicht erbracht hatte. Er informierte die KVB darüber und bat sie um Klärung der Unstimmigkeiten. Nach Überprüfung der vertragsärztlichen Abrechnung teilte die KVB mit, dass sie die unberechtigt vergüteten Leistungen in der Abrechnung mit dem Vertragsarzt korrigiert habe. Zu einer weiteren Information des Auskunftsuchenden sah sich die KVB erklärtermaßen „mangels entsprechender gesetzlicher Befugnis“ nicht berechtigt. Dieser wollte jedoch wissen, welche Kosten für welche ärztlichen Leistungen bei der KVB nun tatsächlich angefallen waren. Mit dem Hinweis, es gehe schließlich nach wie vor um die Frage von ihm in Anspruch genommener ärztlicher Leistungen und deren Kosten, also um seine Sozialdaten, und er könne nicht verstehen, weshalb die KVB insoweit ihm gegenüber die Arztdaten schützen müsse, bat mich der Auskunftsuchende um Überprüfung der KVB-Auffassung.

Ich habe die KVB auf die Auswirkung des § 84 Abs. 1 S. 1 SGB X (Berichtigungspflicht hinsichtlich unrichtiger Daten) und auf die gesetzliche Verpflichtung zur Auskunftserteilung nach § 305 Abs. 1 S. 2 SGB V hingewiesen. Aus § 305 Abs. 1 S. 2 SGB V i.V.m. dem Berichtigungsanspruch nach § 84 Abs. 1 S. 1 SGB X ergab sich die Pflicht der KVB, nach der Berichtigung der unzutreffend gespeicherten Arztabrechnungsdaten auch die entsprechend unzutreffend erteilte Auskunft gegenüber dem Petenten zu berichtigen. Schließlich hatte dieser der KVB die entscheidenden Hinweise gegeben und die Korrekturmitteilung sogar ausdrücklich beantragt.

Einer Korrekturmitteilung an den Versicherten steht nicht entgegen, dass die (korrigierte) Versichertenauskunft Sozialdaten mit einem Doppelbezug aufweist, d. h. auch Sozialdaten des Arztes bzw. Betriebs- und Geschäftsgeheimnisse dieser Arztpraxis mit umfasst. Auf Grund der spezialgesetzlichen Auskunftspflicht der KV nach § 305 Abs. 1 S. 2 SGB V muss es der Arzt hinnehmen, dass der Patient aus der Auskunft bspw. erkennt, wieviel die KV dem Arzt für seine Behandlung bezahlt hat. Ebenso müssen Rückschlüsse auf die Unrichtigkeit der ursprünglichen ärztlichen Abrechnung vom Arzt hingenommen werden, die der Patient aus Korrekturen solcher KV-Auskünfte ziehen kann. Die KVen bzw. der betroffene Arzt können sich insoweit nicht darauf berufen, dass die berichtigte Auskunft etwa wegen „überwiegender berechtigter Interessen“ des Arztes (vgl. § 83 Abs. 4 Nr. 3 SGB X) nicht erteilt werden dürfte. Ein derartiges Interesse des Arztes an einer Geheimhaltung der Datenberichtigung zu Lasten des Auskunftsinteresses des Patienten ist mir gerade für den Fall nicht ersichtlich, dass aus der Korrektur Rückschlüsse auf vom Arzt zwar abgerechnete, aber nicht erbrachte ärztliche Leistungen gezogen werden können.

Aufgrund meiner Hinweise übersandte die KVB dem Versicherten die gewünschte Korrekturmitteilung.

Die KVB ging dabei zu Recht davon aus, dass das Verfahren der Zuleitung einer Versichertenauskunft nach § 305 Abs. 1 S. 1 und 2 SGB V über die Krankenkasse bei einer Korrekturmitteilung nicht mehr eingehalten zu werden braucht. Die beschriebene Verfahrensweise bei der Erstauskunft bezweckt lediglich, dass der Versicherte von der Krankenkasse und damit sozusagen „aus einer Hand“ über die Gesamtheit der im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und deren Kosten unterrichtet wird (ohne dass die Krankenkasse dadurch gleichermaßen umfassende Informationen erhalten würde). Dieser Gesamtauskunft bedarf es

nicht mehr bei einer Korrekturmitteilung, die ausschließlich den KV-Auskunftsbestandteil betrifft.

5.5 Sozialhilfeverwaltung

5.5.1 Sozialbericht und Maßnahmeempfehlung für psychisch kranke/suchtkranke Menschen zur Erstellung eines Gesamtplans gemäß § 46 BHSG; Bildung von Hilfebedarfsgruppen für behinderte Menschen nach dem sog. Metzler-Verfahren

Nach § 46 Bundessozialhilfegesetz (BSHG) hat der Sozialhilfeträger so frühzeitig wie möglich einen **Gesamtplan** zur Durchführung der einzelnen Maßnahmen zur Eingliederung behinderter Menschen aufzustellen. Dadurch sollen die verschiedenen im BSHG vorgesehenen Maßnahmen zur Eingliederung Behinderter in medizinischer, erzieherischer, ggf. auch arbeits- und berufsfördernder Beziehung im Einzelfall festgelegt und aufeinander abgestimmt werden.

Bisher wurde diese Vorschrift in der Praxis nur unvollständig und uneinheitlich umgesetzt. Der Verband der Bayer. Bezirke verfolgt für eine Vereinheitlichung der Verfahrensweise zunächst ein Pilotprojekt Hilfe für den Personenkreis der **(chronisch) psychisch Kranken und Suchtkranken**. Als Instrumente zur Gesamtplanung für jeden einzelnen Behinderten dienen die von einer überregionalen Arbeitsgruppe der Bayer. Bezirke entworfenen Erhebungsbögen „Ärztlicher Bericht / Stellungnahme“ und „Sozialbericht mit Maßnahmeempfehlung“. Anregungen von Fachleuten sowie Einflussnahmen meinerseits führten zu diversen Änderungen und Korrekturen dieser Erhebungsbögen.

Auf Grund von Beschwerden habe ich diese Datenerhebungen nochmals überprüft. Ich bin dabei zu folgenden Ergebnissen gekommen:

Zunächst habe ich entgegen immer wieder erhobener Vorwürfe keine Anhaltspunkte dafür gefunden, dass die Bezirke routinemäßig Informationen über das Sexualverhalten der behinderten Menschen erheben würden. Nur in seltenen Ausnahmefällen, nämlich wenn die Einrichtungen einen hohen Hilfe- bzw. Betreuungsbedarf speziell mit besonderen sexuellen Verhaltensweisen, bspw. dem Risiko sexueller Entgleisungen gegenüber Anderen begründen, fordern die Bezirke

nach den Ergebnissen meiner Anfrage Informationen, die diesen besonderen Hilfe- bzw. Betreuungsbedarf belegen. Das halte ich für sachgerecht.

Im übrigen halte ich die Datenerhebungen für erforderlich und damit für zulässig, wenn ich auch Möglichkeiten für datenschutzrechtliche Verbesserungen sehe. Art, Form und Maß der Sozialhilfe richten sich gemäß § 3 Abs. 1 S. 1 BSHG nach der Besonderheit des Einzelfalls, vor allem nach der Person des Hilfeempfängers, der Art seines Bedarfs und den örtlichen Verhältnissen. Dabei hat nicht die Einrichtung, in der der behinderte Mensch lebt, sondern der zuständige Sozialhilfeträger die Entscheidung über Form und Ausmaß der Sozialhilfegewährung zu treffen. Hierzu benötigt er genaue Kenntnisse über die vorhandenen Fähigkeiten und die auszugleichenden Defizite des Betroffenen. Er muss seine Leistungsentscheidung gegenüber dem einzelnen Betroffenen und gegenüber der steuerzahlenden Allgemeinheit auf Grund sorgfältiger Überprüfung der Voraussetzungen für den Sozialhilfebedarf und für die Sozialhilfeausgaben begründen. Zu berücksichtigen ist auch, dass zwischen Einrichtungsträger und Bezirk durchaus Interessengegensätze bestehen können.

Diese datenschutzrechtliche Einschätzung gilt auch für die Verwendung des **Erhebungsbogens zur Zuordnung von Hilfebedarfsgruppen nach dem sog. „Metzler-Verfahren“**. Ebenfalls in einem Modellversuch erheben die Bezirke diese Bögen personenbezogen für die **durch Verwaltungsakt erfolgende Feststellung** der jeweiligen Hilfebedarfsgruppe gegenüber dem Betroffenen, der in einer stationären Einrichtung für geistig und körperlich behinderte Menschen wohnt. Von der Anerkennung der so ermittelten Hilfebedarfsgruppe hängt die Zahlung der Maßnahmepauschale im Einzelfall ab (als Bestandteil der Vergütung für die Kosten der Einrichtung, vgl. § 93 a Abs. 2 S. 3 BSHG).

Bei meiner datenschutzrechtlichen Bewertung bin ich zu dem Ergebnis gekommen, dass die Mitteilung lediglich der Ergebnisse von Zuordnungen einer der fünf Hilfebedarfsgruppen zu einem behinderten Menschen zwar zur finanziellen Bemessung der Maßnahmepauschalen im Rahmen der Vergütungsneuordnung mit den Einrichtungsträgern (Vergütungsverhandlungen) ausreicht, nicht aber dazu, individuell neue Verwaltungsakte zur Festlegung der qualitativ und quantitativ richtigen Leistungsangebote zu erstellen. Für diese Einzelentscheidung sind auch Einzelangaben erforderlich, die damit nach § 67 a SGB X erhoben und mit Einwilligung des Betroffenen übermittelt werden dürfen. Auch das Arztgeheimnis steht dem dann nicht entgegen.

Sowohl für die Auswertung der Gesamtplanungsinstrumentarien als auch der Erhebungsbögen zur Ermittlung der Hilfebedarfsgruppen nach dem „Metzler-Verfahren“ habe ich aber für ein möglichst schonendes Verfahren Folgendes gefordert:

Im Hinblick auf die Sensibilität der besagten Angaben über die psychisch Kranken bzw. behinderten Menschen halte ich es für erforderlich, dass die sogenannten Fachdienste (Medizinisch-Sozialpädagogische Dienste/MSD) innerhalb der Bezirke baldmöglichst so ausgebaut werden, dass die fachliche Verantwortung und Entscheidungskompetenz für die Beurteilung medizinisch-sozialpädagogischer Voraussetzungen von Sozialhilfeleistungen auf diese Fachdienste übertragen wird, so dass die Erhebungsbögen mit den sensiblen Angaben in diesem nochmals besonders geschützten Bereich dieser Fachdienste verbleiben können.

Inzwischen haben sich auf meine Initiative hin die Bezirke Oberbayern, Mittelfranken und Unterfranken bereit erklärt, in einem Teil der Fälle ihrer Pilotgebiete die fachliche Verantwortung für die Auswertung der Gesamtplaninstrumente den Fachdiensten zu übertragen. In den Bezirken Oberfranken und Unterfranken werden ab August 2002 die Metzler-Erhebungs-Bögen bei Neuaufnahmen nur mehr den Fachdiensten zugeleitet. Ich erwarte, dass die Pilotversuche betreffend die erweiterte Aufgabenübertragung auf die Fachdienste in eine allgemeine Regelung übergehen. Problematisch sind dabei allerdings die Kosten, wobei ich meine, dass die sensible Behandlung dieser Informationen auch gewisse Mehraufwendungen wie vergleichsweise für den Medizinischen Dienst der Krankenversicherung (MDK) rechtfertigt. Außerdem dürfte sich der zusätzliche Personalbedarf beim Fachdienst nach einer Übergangszeit durch einen Personalabbau in der (anderweitigen) Sozialhilfe-Sachbearbeitung der Bezirke zumindest teilweise ausgleichen lassen.

5.6 Jugendämter

5.6.1 Übermittlung im Kindergarten gewonnener Erkenntnisse über individuellen Förderungsbedarf an die aufnehmende Grundschule

U.a. aufgrund der PISA-Studie erreichten mich Anfragen, ob der aufnehmenden Grundschule im Kindergarten gewonnene Erkenntnisse über den individuellen Förderungsbedarf bestimmter Kinder mitgeteilt werden dürfen.

Aus der Sicht des Datenschutzes bestehen diesbezüglich keine Bedenken, wenn die Kindergärten die Schulen mit Einverständnis der Eltern auf entsprechende Probleme der Kinder hinweisen. Dagegen wären solche Hinweise ohne Einverständnis oder sogar gegen den Willen der Eltern nach dem Sozialgesetzbuch - SGB - VIII, dem früheren Kinder- und Jugendhilfegesetz, nicht zulässig. Im einzelnen gilt Folgendes:

Die Zulässigkeit der Übermittlung personenbezogener Daten von Kindergartenkindern an die aufnehmende Grundschule ist gemäß § 61 Abs. 1 und 4 SGB VIII nach den Vorschriften zum Schutz von Sozialdaten zu beurteilen. Dabei muss der besondere Vertrauensschutz in der persönlichen und erzieherischen Hilfe beachtet werden, den § 65 SGB VIII einräumt. Nach dieser Bestimmung dürfen Sozialdaten, die dem Kindergartenpersonal „zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind“, von diesem nur weitergegeben werden „mit der Einwilligung dessen, der die Daten anvertraut hat“, oder „unter den Voraussetzungen, unter denen eine der in § 203 Abs. 1 oder 3 StGB genannten Personen (bspw. ein Arzt, eine staatl. anerkannte Sozialpädagogin usw.) dazu befugt wäre.“

Informationen über den Förderungsbedarf eines Kindergartenkindes, die die Kindergärtnerin aus seinem Verhalten oder seinen Äußerungen gewinnt, sind nach meiner Auffassung anvertraute Sozialdaten in diesem Sinne, soweit es sich nicht um offensichtliche, für jedermann erkennbare Merkmale handelt. Die Eltern bzw. Personensorgeberechtigten haben das Kind dem Kindergarten aus freier Entscheidung anvertraut. Sie ermöglichen bereits auf diese Weise im Vertrauen auf deren besondere Verschwiegenheit den Erzieherinnen und Pflegerinnen, durch intensive Beobachtung, durch an das Kind gerichtete Fragen und Gespräche mit diesem, seine „Stärken und Schwächen“ zu ergründen. Das Kind selbst offenbart sich dem Kindergartenpersonal in aller Regel in „kindlicher Vertrauensseligkeit“. Darüber hinaus ziehen die Sorgeberechtigten ihrerseits das Kindergartenpersonal mit Informationen über Schwächen und Förderungsbedarf des Kindes ins Vertrauen. Dies alles geschieht zum Zweck persönlicher und erzieherischer Hilfe.

Voraussetzungen, unter denen eine in § 203 Abs. 1 oder 3 StGB genannte Person (Arzt etc.) anderweitig als aufgrund einer Einwilligung zur Offenbarung der anvertrauten Daten berechtigt wäre (bspw. bei rechtfertigendem Notstand), sehe ich im vorliegenden Zusammenhang nicht. Damit dürfen diese Daten nur mit Einwilligung der Eltern bzw. Personensorgeberechtigten an die Grundschule weitergegeben werden.

Soweit es sich beim Kindergartenpersonal um staatlich anerkannte Sozialpädagogen/innen handelt, die einem besonderen Berufsgeheimnis unterliegen, sowie um ihre berufsmäßig tätigen Gehilfen und ihre Auszubildenden, ist § 203 StGB nicht nur nach Maßgabe von § 65 SGB VIII zu beachten, sondern gilt als Strafnorm für diesen Personenkreis unmittelbar. Für ihn bedarf es also zur Offenbarung personenbezogenen Förderungsbedarfs einzelner Kinder gegenüber der Grundschule auch im Hinblick auf das Strafgesetzbuch der Einwilligung.

Dieser Rechtslage wird die Bekanntmachung des Staatsministeriums für Unterricht und Kultus vom 29.06.1998 zur Zusammenarbeit zwischen vorschulischen Einrichtungen und Grundschule gerecht, wo unter Ziff. 3 Folgendes ausgeführt wird: „Da die Erzieher aufgrund einer langfristigen und ganzheitlichen Beobachtung den Entwicklungsstand eines Kindes kennen, sind sie bei Fragen der Schulfähigkeit bzw. eines individuellen Förderbedarfs im Sinne einer Entscheidungshilfe zu hören, sofern die Personensorgeberechtigten zustimmen.“ In den vom Sozialministerium herausgegebenen „Empfehlungen zur Umsetzung der Verordnung über die Rahmenpläne für anerkannte Kindergärten (4. DVBayKiG) in der Praxis“ befindet sich übrigens eine Darstellung diverser weiterer Möglichkeiten zur Ausgestaltung dieser Zusammenarbeit.

Ich meine, es ist auch im Sinne der Kinder, dass die wohl unstreitig wichtige und durchaus begrüßenswerte enge Zusammenarbeit zwischen Kindergarten und Grundschule durch Information der Schule über den besonderen Förderungsbedarf einzelner Kindergartenkinder nicht an den Eltern vorbei, sondern vielmehr mit deren Wissen und Wollen, also mit deren Einwilligung geschieht.

5.7 Unfallversicherung

5.7.1 Recht der Unfallversicherten zur Auswahl eines Gutachters nach § 200 Abs. 2 SGB VII

Immer wieder zeigt sich, dass die Unfallversicherungsträger (UVT) dem Gutachterauswahlrecht nach § 200 Abs. 2 SGB VII zuungunsten der Versicherten nicht angemessen Rechnung tragen. Nach dieser Vorschrift sind die UVT regelmäßig verpflichtet, dem Versicherten „mehrere“, d.h. mindestens drei Gutachter zur Auswahl zu benennen. Mit dieser Regelung hat der Gesetzgeber eine Verbesserung der Mitwirkungsrechte des Versicherten und eine gesteigerte Transparenz des Begutachtungsverfahrens bezweckt. Nicht zuletzt von Seiten des Datenschutzes ist daher darauf

zu achten, dass die Intentionen des Gesetzgebers in der Praxis der UVT und auch der Gutachter nicht ausgehöhlt werden. Dem Gutachterauswahlrecht wird bspw. nicht Genüge geleistet, wenn der Versicherte erst bei seinem Erscheinen am Untersuchungstag bzw. -ort von einem untersuchenden Arzt darüber informiert wird, dass nunmehr ein anderer als der vom Versicherten ausgewählte Gutachter die Begutachtung durchführen bzw. verantworten werde, weil der ausgewählte dazu - aus welchen Gründen auch immer - nicht in der Lage sei.

Das Gutachterauswahlrecht wird insbesondere bei der Einschaltung von Zusatzgutachtern durch den (ausgewählten) Hauptgutachter nicht angemessen beachtet. Oftmals stellt dieser erst nach Aufnahme der Hauptbegutachtung die Notwendigkeit von Zusatzgutachten fest und zieht seinerseits Zusatzgutachter hinzu. Die vom Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) vertretene Rechtsauffassung, wonach es hinsichtlich § 200 Abs. 2 SGB VII ausreiche, wenn der UVT dafür Sorge trage, dass die beauftragten Hauptgutachter die Versicherten über die im Rahmen des Gutachtenauftrags zusätzlich tätig werdenden Ärzte informieren und insofern Einvernehmen mit den Versicherten herstellen, überzeugt angesichts des vom Gesetzgeber eindeutig zugunsten der Versicherten geschaffenen Gutachterauswahlrechts nicht.

Im Hinblick auf die Verantwortung der UVT für die Ausgestaltung des Begutachtungsverfahrens erscheint es mir als datenschutzrechtlich erforderlich (aber auch ausreichend), dass sie zur Sicherstellung des Gutachterauswahlrechts bei der von Hauptgutachtern betriebenen Einschaltung von Zusatzgutachtern die beauftragten Hauptgutachter vertraglich dazu verpflichten, erforderliche **Zusatzbegutachtungen nur in Abstimmung mit dem Versicherten und nur unter Berücksichtigung des Gutachterauswahlrechts nach § 200 Abs. 2 SGB VII** in Auftrag zu geben. Ebenfalls vertraglich vorzusehen ist, dass die Begutachtungsstelle den UVT über die vorgesehene Zusatzbegutachtung und die hierfür zur Auswahl gestellten Gutachter in Kenntnis setzt, damit er seine Einflussmöglichkeiten auf das Begutachtungsverfahren wahrnehmen und damit z.B. die Datenübermittlung an ungeeignete Gutachter verhindern kann. Die Begutachtungsstelle hat außerdem den Versicherten darauf hinzuweisen, dass er die Gutachtervorschläge und seine Auswahl statt mit dem Hauptgutachter auch mit dem UVT erörtern und seine Erklärung ihm gegenüber abgeben kann.

Erst wenn die Person des Zusatzgutachters feststeht und der Betroffene nicht nach den §§ 200 Abs. 2 SGB VII i.V.m. 76 Abs. 2 SGB X widersprochen hat, dürfen Sozialdaten des Versicherten an den Zusatzgutachter weitergegeben werden.

Die Bau-Berufsgenossenschaft Bayern und Sachsen hat auf meine Forderung zugesagt, so zu verfahren.

Leider hat der Gesetzgeber in § 200 Abs. 2 SGB VII bisher nicht direkt zum Ausdruck gebracht, dass die Unfallversicherten über ihr Gutachterauswahlrecht hinaus berechtigt sind, selbst einen oder mehrere Gutachter vorzuschlagen. Diese Berechtigung lässt sich aber jedenfalls aus der Gesetzesbegründung entnehmen. Das Gutachtervorschlagsrecht der Versicherten wird mittlerweile zwar von vielen UVT nicht mehr bestritten, es bestehen aber noch Umsetzungsdefizite:

- Die UVT verhalten sich inkonsequent, indem sie einerseits dieses Vorschlagsrecht der Versicherten grundsätzlich akzeptieren, es andererseits aber dadurch weitgehend leer laufen lassen, dass sie mangels ausdrücklicher Regelung in § 200 Abs. 2 SGB VII nicht auf diese Berechtigung hinweisen. Bereits aufgrund der allgemeinen Vorschrift des § 14 SGB I hat jedoch ein Jeder Anspruch auf Beratung über seine Rechte und Pflichten nach dem Sozialgesetzbuch.
- Außerdem betrachten die meisten UVT Gutachtervorschläge des Versicherten als unverbindlich. Das Bundesministerium für Arbeit und Soziales hat dem Bundesbeauftragten für den Datenschutz aber bestätigt, dass die UVT nachvollziehbar begründen müssen, warum sie dem Gutachtervorschlag eines Versicherten ggf. nicht folgen.

5.7.2 Beanstandung einer Berufsgenossenschaft wegen Weitergabe personenbezogener Gesundheitsdaten an ein Chemie-Unternehmen

In unfallversicherungsrechtlichen Verwaltungsverfahren zur Feststellung, ob bspw. eine Hautkrankheit oder eine toxische Leberschädigung als Berufskrankheit anzuerkennen ist, erfragen Berufsgenossenschaften bei den Herstellern vielfach die Zusammensetzung chemischer Produkte, mit denen der Betroffene bei seiner Erwerbstätigkeit in Berührung gekommen ist. Ein Chemie-Unternehmen hat mir berichtet, dass eine bestimmte Berufsgenossenschaft (BG) hierzu die betroffenen Versicherten mit Name und Adresse und jedenfalls in manchen Fällen sogar unter Angabe der in Betracht kommenden Berufskrankheit und des Arbeitgebers benenne. Dies sei leider das Standardverfahren bei dieser BG.

Die betroffene BG hat diesen Sachverhalt auf Nachfrage bestätigt und gleich eingeräumt, dass die personenbezogene Übermittlung aller genannten und schließlich ja auch gesundheitsrelevanten Daten der betroffenen Versicherten für Anfragen an Produkthersteller nicht erforderlich und deshalb unzulässig ist. Die BG hat diese Datenschutzverstöße ausdrücklich bedauert und ihre Bediensteten angewiesen, die Angabe der Sozialdaten bei solchen Anfragen sofort einzustellen.

Ich habe die BG beanstandet. Ich meine, ein derart unbedachter und unsensibler Umgang mit identifizierenden gesundheitlichen Daten durch die Sachbearbeitung ist absolut nicht mehr zeitgemäß und dürfte auf eine jedenfalls vor meiner Intervention unzureichende Mitarbeiterschulung über den Sozialdatenschutz zurückzuführen sein.

6 Polizei

Meine Tätigkeit im Polizeibereich umfasste die Kontrolle von **Speicherungen in Dateien und Karteien**, wie z. B. im Kriminalaktennachweis der Bayerischen Polizei (KAN), in der Geldwäschedatei, der Arbeitsdatei „Rauschgift“, der Fahndungsdatei einer Polizeidirektion, der Staatsschutzdatei Bayern sowie in weiteren Dateien, insbesondere in regional geführter GAST-Dateien, und von **Datenerhebungsmaßnahmen** wie Identitätsfeststellungen und erkennungsdienstliche Behandlungen. Die Rasterfahndung nach den Terroranschlägen am 11. September 2001 in den USA, Maßnahmen zum Zwecke der DNA-Analyse sowie Videoaufnahmen auf Versammlungen und auf öffentlichen Straßen und Plätzen bildeten weitere Prüfungsschwerpunkte.

Geprüft habe ich auch wieder **Datenübermittlungen** der Polizei, z. B. an die Presse, an Fahrerlaubnisbehörden und an Gesundheitsämter, **Abfragen in Informationssystemen** durch Polizeibedienstete sowie die **Auskunftserteilung an Betroffene** über polizeiliche Speicherungen.

Neben meiner Kontrolle vorgenannter Datenerhebung, -nutzung und -verarbeitung durch die Polizei aufgrund von Bürgereingaben, Pressemitteilungen oder sonstigen Hinweisen habe ich anlassunabhängig wieder mehrere Prüfungen bei verschiedenen bayerischen Polizeidienststellen vorgenommen.

Des Weiteren habe ich durch datenschutzrechtliche Beurteilungen auf eine datenschutzkonformen Realisierung von **Gesetzen und Richtlinien** hingewirkt, welche Eingriffe in das informationelle Selbstbestimmungsrecht durch die Polizei zum Gegenstand hatten. Insbesondere habe ich zahlreiche Errichtungsanordnungen für Dateien überprüft und an Prüfungen für bundesweite Dateien mitgewirkt.

Meine datenschutzrechtliche Beratung von Polizeidienststellen umfasste auch Vorträge bei Aus- und Fortbildungsveranstaltungen der Polizei.

Die nachfolgenden Darstellungen sind eine Auswahl meiner Feststellungen im Polizeibereich.

6.1 Kriminalaktennachweis (KAN)

In meinem 19. Tätigkeitsbericht (vgl. Nr. 5.3.1.1) hatte ich vom vorläufigen Ergebnis meiner Verhandlungen mit dem Innenministerium zur datenschutzrechtlichen Verbesserung des Verfahrens der personenbezogenen Speicherung von Erkenntnissen aus strafrechtlichen Ermittlungsverfahren insbesondere im Kriminalaktennachweis berichtet. In dieser Datei, die von allen bayerischen Polizeibeamten und von bevollmächtigten Polizeiangestellten abgerufen werden kann, dürfen grundsätzlich Beschuldigte, aber auch Personen gespeichert werden, bei denen die Beschuldigteneigenschaft entfallen ist, soweit der Tatverdacht fortbesteht. Ist der Tatverdacht entfallen, darf keine Speicherung im KAN erfolgen bzw. ist eine schon erfolgte Speicherung zu löschen. Die von mir festgestellten Defizite bezogen sich in erster Linie auf den Zeitpunkt der Prüfung des Tatverdachts und die zu enge Definition von Fällen geringerer Bedeutung.

Die auf meine Forderungen vom Staatsminister des Innern in Aussicht gestellte Änderung der Vorschriftenlage wurde nunmehr bis zur Neufassung der Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien) und der Errichtungsanordnung für die Personen- und Fall-Auskunftsdatei (EA PFAD) in Form einer Übergangsregelung umgesetzt. Danach erfolgt die Prüfung der Speicherungsfrist nicht nur bei Einleitung der polizeilichen Ermittlungen sondern auch nach deren Abschluss. Eine erneute Prüfung hat zu erfolgen, wenn bei Rücklauf eines Vorgangs von der Verfolgungsbehörde erkennbar ist, dass diese weitere Ermittlungen mit entlastenden Erkenntnissen vorgenommen hat. Dies gilt insbesondere auch für Pri-

vatklage- und Fahrlässigkeitsdelikte. Damit wird einem Teil meiner wesentlichen Forderungen Rechnung getragen.

Bei Fällen geringerer Bedeutung ist nun ebenfalls eine Verbesserung eingetreten, soweit der nunmehr eröffnete Entscheidungsspielraum von den einzelnen Polizeibeamten auch genutzt wird. Nach der neuen Vorschriftenlage ist die Vergabe kürzerer Aufbewahrungsfristen als die Regelfristen des Art. 38 Abs. 2 Satz 3 PAG nicht mehr nur bei den bisher abschließend genannten Delikten möglich. Bei der Festsetzung einer verkürzten Speicherungsfrist ist eine strenge einzelfallbezogene Bewertung von Tat und Täter durch den Sachbearbeiter entscheidend. Die Gründe hierzu sind zu dokumentieren.

Die oben genannten Änderungen gehen in die richtige Richtung, sie gehen aber nicht weit genug. Da die Erforderlichkeit einer Speicherung aufgrund der polizeilichen Ermittlung entfallen kann, sollte ausdrücklich auf die entsprechende Prüfungsverpflichtung der Polizei hingewiesen werden. Andernfalls besteht die Gefahr, dass die Notwendigkeit einer solchen Prüfung nicht gesehen und die Prüfung auf die Speicherungsdauer beschränkt wird. Ich habe deshalb folgende Ergänzung vorgeschlagen: „Grundsätzlich erfolgt eine abschließende ***Prüfung*** und Festlegung, ***ob eine Speicherung zur polizeilichen Aufgabenerfüllung erforderlich ist*** sowie der Aussonderungsprüffrist nach Abschluss der polizeilichen Ermittlungen.“ Des Weiteren habe ich gefordert, für eine Fristverkürzung keine „***strenge***“ Einzelfallprüfung vorzuschreiben. Dadurch könnte der Gefahr entgegengewirkt werden, dass die Bereitschaft von Fristverkürzungen Gebrauch zu machen, unvertretbar herabgesetzt wird. Diese Gefahr würde aber bestehen, wenn neben den Regelfristen in Art. 38 PAG und einer Dokumentationsverpflichtung auch noch ein strenger Maßstab für die Fristverkürzung vorgegeben wird.

Das Staatsministerium des Innern hat meine Vorschläge leider abgelehnt. Die von mir vorgeschlagene „Prüfung“ der Erforderlichkeit der polizeilichen Speicherung sei an dieser Stelle systemfremd. Der Erforderlichkeitsgrundsatz ziehe sich wie ein roter Faden durch die Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (RPpS), so dass ein eigener Hinweis insbesondere bei den Regelungen zu den Aufbewahrungs- (Speicherungs-)Fristen und zur Aussonderung/Löschung als entbehrlich erachtet werde. Auch meiner Anregung nach Streichung des Wortes „strenger“ könne es nicht nachkommen. Die Gefahr einer unvertretbaren Herabsetzung der Bereitschaft zur Fristverkürzungen sei für das Innenministerium nicht erkennbar. Es sehe aufgrund der Öffnung des Deliktsspektrums für die Vergabe kürzerer Speicherfristen viel-

mehr eine gesteigerte Verpflichtung für einen Hinweis auf eine strenge Einzelfallprüfung, um Fehlbeurteilungen und darauf beruhenden möglichen Gefährdungen des Sicherheitszustandes durch einzelne Tatverdächtige vorzubeugen. In diesem Zusammenhang wurde an einen Mordfall erinnert, bei dem der mutmaßliche Täter lediglich mit Kfz-Delikten in Erscheinung getreten war.

Meine Forderung, auf die Verpflichtung zur Prüfung der Erforderlichkeit in den Richtlinien hinzuweisen, halte ich aufrecht. Ein solcher Hinweis dient der Klarstellung, dass sich diese Verpflichtung gerade und besonders auf den Zeitpunkt des Abschlusses der polizeilichen Ermittlungen bezieht.

Die Begründung für die ablehnende Haltung des Innenministeriums gegenüber eine ausgewogenen Beurteilung des Vorliegens von Fällen geringerer Bedeutung halte ich für wenig überzeugend. Würde man ihr folgen, käme grundsätzlich kein Delikt als Fall geringerer Bedeutung in Betracht, da auch ein „Ladendieb“, „Schwarzfahrer“ oder „Beleidiger“ Täter eines späteren Sexualmordes werden kann und seine langfristige Speicherung zur Aufklärung eine solchen Tat beitragen könnte. Eine entsprechende (fehlerhafte) Vorstellung könnte auch bei polizeilichen Sachbearbeitern (Entscheidern) entstehen und durch die Formulierung „strenge Prüfung“ noch nachhaltig unterstützt werden. Bei der durchzuführenden Einzelfallprüfung darf aber nicht auf völlig ungewisse und in den allermeisten Fällen auch nicht eintreffende Folgedelikte abgestellt werden. Die Prüfung sollte deshalb nicht „streng“ sondern objektiv, aufgaben- und datenschutzkonform durchgeführt werden.

Auch einer weiteren Forderung, die ich bereits im Zuge meiner Feststellungen bei der Schwerpunktprüfung 1998 an das Innenministerium herangetragen hatte, wurde leider nicht entsprochen. Danach sollten Speicherungen auch nach Verfahrenseinstellungen gemäß §§ 153 ff. StPO, 45, 47 Jugendgerichtsgesetz (z. B. wegen Geringfügigkeit, geringer Schuld und fehlendem öffentlichen Interesse an der Strafverfolgung) erneut überprüft werden, da eine solche Verfahrensbeendigung zumindest eine Bewertung der Tat als Fall geringerer Bedeutung mit verkürzter Speicherungsfrist nahelegt. Eine solche Prüfung halte ich nach wie vor für erforderlich.

Die Notwendigkeit einer sorgfältigen polizeilichen Prüfung von Speicherungen machen folgende Beispiele deutlich: Ein Bürger hat sich an mich gewandt, weil er ohne ersichtlichen Anlass zu einer Verkehrskontrolle angehalten und im Rahmen des Kontrollvorgangs danach gefragt wurde, ob er vor kurzem schon einmal mit der Polizei zu tun gehabt habe. Ich habe daraufhin die poli-

zeilichen Speicherungen überprüft und festgestellt, dass im Zusammenhang mit einer früheren Verkehrskontrolle Speicherungen wegen Trunkenheit im Verkehr und Widerstands gegen Vollstreckungsbeamte zu seiner Person vorhanden waren. Damals hatten die Beamten den Verdacht, dass der Betroffene alkoholisiert gewesen sei. Außerdem war es im Rahmen der Kontrolle offenbar zu einem Handgemenge gekommen, in dessen Verlauf der Betroffene „zu Boden gebracht“ und gefesselt worden war, nachdem er versucht hatte, seinen auf der Motorhaube des Polizeifahrzeugs liegenden Führer- und Fahrzeugschein wieder an sich zu nehmen und diesen Versuch trotz anderslautender Aufforderung der Polizeibeamten fortsetzte.

Die Blutalkohol und Urinuntersuchung hatte jedoch ergeben, dass weder eine Alkoholbeeinflussung vorgelegen hatte, noch Arznei- oder Suchtmittel eingenommen worden waren. Das Verfahren wegen des Vorwurfs der Trunkenheit im Verkehr wurde daher von der Staatsanwaltschaft wegen erwiesener Unschuld eingestellt. Auch das Verfahren wegen Widerstands gegen Vollstreckungsbeamte stellte die Staatsanwaltschaft wegen geringer Schuld und mangelndem öffentlichen Interesse mit der Begründung ein, es habe nur eine geringfügige Widerstandshandlung vorgelegen, die im Zusammenhang mit dem harten Vorgehen der beteiligten Polizeibeamten gestanden habe.

Trotzdem wurden beide Tatvorwürfe von der Polizei unzulässigerweise weiterhin im KAN gespeichert.

Mit Kenntnis des Untersuchungsergebnisses hätte die Speicherung wegen Trunkenheit im Verkehr gelöscht werden müssen, da sie für den polizeilichen Sachbearbeiter erkennbar rechtswidrig war. Hinsichtlich des Vorwurfs des Widerstands gegen Vollstreckungsbeamte ergab sich die Löschungsverpflichtung zwar nicht bereits aus der Einstellung des Strafverfahrens durch die Staatsanwaltschaft. Allerdings ist für jede Speicherung die konkrete Erforderlichkeit unter Beachtung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit zu berücksichtigen. Zu fragen ist also jeweils anhand der Umstände des Einzelfalles, ob trotz Einstellung des Verfahrens nach kriminalistischer Erfahrung weiterhin Anhaltspunkte dafür bestehen, dass die betreffende Person künftig strafrechtlich in Erscheinung treten wird, so dass die angefertigten Unterlagen dann die Ermittlungen der Polizei fördern können. Daran fehlte es hier jedoch aufgrund der Tatumstände, wie sich auch aus der Einstellungsbegründung der Staatsanwaltschaft ergab.

Diese gravierenden datenschutzrechtlichen Verstöße habe ich förmlich beanstandet. Im Zuge meiner Überprüfung bzw. Beanstandung wurden beide Speicherungen gelöscht.

Einen weiterer Fall zeigt die schwerwiegenden Folgen einer fehlerhaften Speicherung für die Betroffene: Aufgrund eines Erfassungsfehlers bei einer Polizeidienststelle - es wurde eine Ziffer der Kriminalaktennachweisnummern vertauscht - wurde eine nicht gesuchte Bürgerin im Fahndungssystem zur Festnahme ausgeschrieben. Aufgrund dieser Ausschreibung wurde die Frau von der Polizei festgenommen, erkennungsdienstlich behandelt und blieb für mehrere Stunden bis zur Aufklärung des Missverständnisses in der Haftanstalt des Polizeipräsidiums inhaftiert. Der Fehler wäre m.E. bei entsprechender Sorgfalt zu vermeiden gewesen. Wegen der schweren Folgen für die Bürgerin und der damit verbundenen psychischen Belastung habe ich die fehlerhafte Speicherung förmlich beanstandet.

Im Berichtszeitraum habe ich anlässlich von Bürgereingaben und Prüfungen bei Polizeidienststellen mehrfach festgestellt, dass die Deliktsbezeichnung im Kriminalaktennachweis fehlerhaft war. Dies lag in allen Fällen daran, dass die Anzeige bei der Polizei z. B. wegen Vergewaltigung oder Körperverletzung erfolgte, durch die Justiz aber festgestellt wurde, dass es sich bei der Vergewaltigung um eine Körperverletzung, bei der Körperverletzung um eine Beleidigung gehandelt hatte. Diese abweichende rechtliche Einordnung der Justiz wurde von der Polizei nicht berücksichtigt. Sie wäre aber verpflichtet gewesen, spätestens bei der Mitteilung des Verfahrensausgangs durch die Justiz, von welcher der Sachbearbeiter Kenntnis nehmen sollte, die dort getroffenen Feststellungen zum Anlass zu nehmen, die Deliktsbezeichnung entsprechend zu berichtigen. So macht es einen erheblichen Unterschied, wenn bei einer polizeilichen Kontrolle die Abfrage des Kriminalaktennachweises Vergewaltigung statt Körperverletzung oder Körperverletzung statt Beleidigung ergibt. In den von mir festgestellten Fällen wurden die Deliktsbezeichnungen auf meine Aufforderung hin berichtigt.

6.2 Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)

In meinem 19. Tätigkeitsbericht (Nr. 5.4.1) hatte ich von einer personenbezogenen Lagedatei berichtet, auf die alle Beschäftigten eines Polizeipräsidiums Zugriff erhalten sollten. Diese Datei ist zwischenzeitlich mit abgestuften Zugriffsberechtigungen realisiert. Leider musste ich feststellen, dass sich die Tendenz zu erweiterten, regional übergreifenden Zugriffsmöglichkeiten auf

polizeiliche Dateien nachhaltig fortsetzt. So habe ich erst im Rahmen eines Gesprächs Ende 2000 erfahren, dass das Staatsministerium des Innern bereits im Oktober 1999 den Zugriff auf die vormals regional geführten Dateien PSV präsidiumsweit eröffnet hat. Bis dahin war das nur in den Ballungsraumpräsidien München und Mittelfranken der Fall. Das Innenministerium hat mich von sich aus weder vor noch nach dieser Erweiterung darüber informiert, obwohl es sich um eine Änderung von wesentlicher datenschutzrechtlicher Bedeutung handelt.

Abgesehen von der mangelnden Information durch das Innenministerium habe ich Zweifel an der Erforderlichkeit der Zugriffserweiterung. Anfang der 90er-Jahre war der sog. Regional-KAN mit präsidiumsweitem Zugriff aufgelöst worden. Regionale Ereignisse (z. B. Straftaten von geringerer Bedeutung als Ersterkenntnis, Verkehrsunfälle, Ordnungswidrigkeiten von nicht erheblicher Bedeutung, Ruhestörungen, Fund- oder Verlustanzeigen etc.), insbesondere auch die personenbezogenen Daten von Anzeigeerstatter, Zeugen, Geschädigten sollten nur noch in regionalen Dateien (PSV) gespeichert werden, während insbesondere sonstige Straftaten im bayernweiten Kriminalaktennachweis (vgl. Nr. 6.1) gespeichert werden können. Diese sinnvolle Differenzierung entsprechend der sachlichen Bedeutung wurde nunmehr durch die Erweiterung des Zugriffs auf die PSV aufgehoben, die auch der Schutzbedürftigkeit besonders sensibler Daten, wie der von Opfern (z. B. Geschädigte von Sexualdelikten), nicht Rechnung trägt.

Das Innenministerium hat bisher trotz wiederholter Aufforderung keine für diese massive datenschutzrechtliche Verschlechterung befriedigende Begründung abgegeben.

Verschärft wird die dargestellte Problematik präsidiumsweiter Zugriffe durch überlange Aussonderungsprüffristen bei der Speicherung personenbezogener Daten sog. Dritter, wie z. B. Geschädigte, Anzeigeerstatter, Hinweisgeber in bestimmten Fällen. Zwar werden personenbezogene Daten in der PSV grundsätzlich nur fünf Jahre gespeichert, nicht aber bei Vorgängen, die auch im Kriminalaktennachweis gespeichert sind. In diesem Fall richtet sich die Speicherungsdauer nicht nur für den Täter oder Tatverdächtigen sondern auch für den Dritten nach der Dauer der Speicherung des Vorgangs im Kriminalaktennachweis. Das sind bei der Speicherung von Daten Erwachsener regelmäßig zehn Jahre. Diese Fristen können sich durch die sog. Mitzieh-Automatik des Art. 38 Abs. 2 Satz 6 Polizeiaufgabengesetz um Jahre oder gar Jahrzehnte verlängern, wenn innerhalb der Frist weitere Speicherungen für den Täter oder Tatverdächtigen hinzukommen. So könnte z. B. das Opfer einer Sexualstraftat, die schon Jahrzehnte zurückliegt, immer noch in der PSV gespeichert werden. Dies halte ich für nicht erforderlich und deshalb für

unzulässig. Zu Dokumentations- und Verwaltungszwecken halte ich eine fünfjährige Speicherungsfrist für personenbezogenen Daten Dritter für ausreichend. Werden die Daten ausnahmsweise nach Löschung in der PSV benötigt, können sie der Kriminalakte des Täters/Tatverdächtigen entnommen werden.

Zur Speicherungsdauer von Daten Dritter hat das Staatsministerium des Innern nach 16 Monaten und meiner Aufforderung, die unzulässige Verlängerung der Speicherungsfrist für personenbezogene Daten Dritter einzustellen, einen Änderungsvorschlag unterbreitet. Danach soll sich die Speicherungsdauer für personenbezogene Daten Dritter grundsätzlich nach der Regelfrist des Art. 38 Abs. 2 Satz 3 PAG für die Speicherung von Kriminalakten richten, d. h. zehn Jahre bei Erwachsenen, fünf Jahre bei Jugendlichen und zwei Jahre bei Kindern. Bei Fällen von geringerer Bedeutung und Vorgängen, die nicht in Kriminalakten nachgewiesen sind, wäre die Speicherungsdauer grundsätzlich fünf Jahre, eine Verlängerung der Speicherung aufgrund der o. g. Mitzieh-Automatik soll für gespeicherte Daten Dritter entfallen. Allerdings sollen diese Speicherungen für weitere fünf Jahre verlängert werden können, wenn innerhalb der letzten fünf Jahre vor Fristende des Vorgangs dieser erneut eine Sachbearbeitung erforderlich macht.

Diesen Vorschlag halte ich grundsätzlich für diskussionsfähig, wenn ich auch eine Reduzierung der Frist von zehn Jahren auf fünf Jahre für angemessen gehalten hätte. Allerdings sollte eine Verlängerung der Speicherungsfrist bei erneuter Sachbearbeitung nicht automatisch sondern erst nach Prüfung erfolgen, ob die erneute Sachbearbeitung im konkreten Einzelfall eine Fristverlängerung rechtfertigt. Dies habe ich dem Innenministerium mit der Bitte um Berücksichtigung mitgeteilt.

6.3 Speicherungen im Zusammenhang mit der Münchner Sicherheitskonferenz

Vom 1. bis 3. Februar 2002 fand in München die 38. NATO-Sicherheitskonferenz statt, aus deren Anlass sich NATO-Vertreter und Sicherheitsexperten in einem Hotel in der Münchner Innenstadt trafen. Bereits im Vorfeld hatten die Sicherheitsbehörden Sicherheitsstörungen befürchtet. Hierzu wurde auf konkrete Erkenntnisse von Polizei und Nachrichtendiensten sowie auf die Störungen bei ähnlichen Veranstaltungen wie in Genua und Salzburg verwiesen. Als eine der Maßnahmen zur Verhütung derartiger Störungen hatte die Stadt München eine angekündigte Versammlung, die sich u. a. gegen Themen der Konferenz richten sollte, verboten.

Trotz des Demonstrationsverbots versammelten sich zahlreiche überwiegend junge Menschen in der Innenstadt. Im Verlauf dieser „Kundgebung“ kam es zur Festnahme und Gewahrsamnahme von ca. 800 Personen. Die polizeilichen Maßnahmen waren nach Mitteilung der Polizei wegen der Verfolgung von Straftaten und Ordnungswidrigkeiten und zur Gefahrenabwehr erfolgt.

Bereits unmittelbar nach den Vorfällen habe ich begonnen, insbesondere die Speicherung der personenbezogenen Daten der von den polizeilichen Maßnahmen betroffenen Personen datenschutzrechtlich zu prüfen. Ich habe mit der Polizei vereinbart, dass mir das für die Speicherung der Daten dieser Personen vorgesehene Konzept vorgelegt wird, in dem festgelegt werden sollte, welcher Personenkreis in welcher Datei mit welcher Frist und nach welchen Kriterien gespeichert wird. Das mir übersandte Konzept sieht vor, dass die betroffenen Personen in verschiedene Kategorien eingeteilt werden, insbesondere danach, ob die Personen Straftaten oder Ordnungswidrigkeiten begangen haben, ob einschlägige Vorerkenntnisse vorhanden sind oder ob die Gewahrsamnahme aus rein präventiven Gründen erfolgt ist. Die Einteilung in die jeweilige Kategorie ist ausschlaggebend dafür, wer wie lange in welcher Datei gespeichert wird.

Gegen dieses Speicherungskonzept habe ich in wesentlichen Punkten Einwände erhoben. Insbesondere habe ich mich gegen die Absicht gewandt, Personen, die in Gewahrsam genommen wurden, ohne dass weitere Speicherungsgründe vorliegen, für den allgemeinen polizeilichen Zugriff in der Vorgangsverwaltungsdatei (PSV) zu speichern. Die Speicherung ist zwar zur Dokumentation der polizeilichen Maßnahmen befristet erforderlich. Wegen des allgemeinen Zugriffs und der Doppelfunktionalität der Datei PSV (Vorgangsverwaltung/polizeiliche Präventionsdatei) sehe ich aber eine besondere Belastung für die gespeicherten Personen. Die Speicherung und der präsidiumsweite Zugriff auf die gespeicherten Daten bergen die Gefahr, dass junge Menschen, die sich keine Straftat oder Ordnungswidrigkeit zu Schulden haben kommen lassen, durch Nutzung und Verarbeitung ihrer Daten in großer Zahl zumindest in die Nähe des politischen Extremismus gerückt werden und dadurch Schaden erleiden könnten. Da eine Trennung von Prävention und Vorgangsverwaltungsfunktion bei der Datei PSV nicht möglich ist, sollten die Speicherungen für den allgemeinen Zugriff zumindest gesperrt werden.

Weiterhin habe ich der Absicht widersprochen, dass Personen, denen keine Straftat sondern nur Ordnungswidrigkeiten nach dem Versammlungsgesetz vorgeworfen werden (z. B. die Teilnahme an der verbotenen Versammlung) im Kriminalaktennachweis (vgl. Nr. 6.1) gespeichert werden

sollen, wenn über diese bereits Staatsschutzkenntnisse vorliegen bzw. wenn diese als Aktivisten (Aufwiegler, Anheizer, Flugblattverteiler) aufgefallen sind. Die Speicherung einer Ordnungswidrigkeit im Kriminalaktennachweis als Ersterkenntnis widerspricht den eigenen Speicherungsrichtlinien der Polizei, die grundsätzlich von schwerwiegenden Ordnungswidrigkeiten ausgehen oder jedenfalls fordern, dass die Aufnahme zur Gefahrenabwehr erforderlich ist. Diese Voraussetzungen sehe ich bei nur einer leichten Ordnungswidrigkeit nicht als gegeben an. Auch beabsichtigte Speicherungen in weiteren Dateien habe ich kritisiert.

Die Polizei hat es leider abgelehnt, das Speicherungskonzept entsprechend meinen Forderungen zu modifizieren. Ich habe mich deshalb an das Innenministerium mit der Bitte um Abhilfe gewandt. Eine Antwort steht noch aus.

Unabhängig vom weiteren Ergebnis der noch nicht abgeschlossenen Diskussion beabsichtige ich, die Speicherungen von Personen im Zusammenhang mit der Münchner Sicherheitskonferenz im kommenden Jahr eingehend vor Ort zu prüfen.

6.4 Speicherungen im Zusammenhang mit einer Greenpeace-Aktion

Bereits 1996 wurden die personenbezogenen Daten von ca. 20 Beteiligten an einer Greenpeace-Aktion vor der Staatskanzlei von der Polizei wegen Nötigung und/oder Verstoßes gegen das Uniformverbot nach dem Versammlungsgesetz im Kriminalaktennachweis (vgl. Nr. 6.1) gespeichert. Nach dem zugrundeliegenden Sachverhalt hatten Greenpeace-Aktivisten, zum Teil mit weißen Overalls mit und ohne Aufschrift „Greenpeace“, die Haupttür zur Staatskanzlei durch Ketten mit Schlössern für ca. zehn Minuten versperrt. Auf Verlangen hatte der Leiter der Aktion den Schlüssel jedoch ohne Widerstand herausgegeben. Vier namentlich nicht feststehende Personen hatten aufgrund der zeitlich nicht begehbaren Haupttür seitlich gelegene Notausgänge benutzen müssen.

Das Bayerische Oberste Landesgericht bestätigte mit seinem Urteil vom 16.12.1999 die Entscheidung des Amtsgerichts München vom 13.02.1998, wonach kein Verstoß gegen das Uniformverbot vorlag. Die Polizei löschte daraufhin die entsprechende Speicherung im KAN, die Speicherung wegen Nötigung wurde aufrechterhalten. Insoweit sei das Verfahrens gemäß § 153 Abs. 1 Strafprozessordnung eingestellt worden, was den Tatverdacht gegen die Betroffenen fort-

bestehen lasse. Dieser Auffassung habe ich widersprochen, da ich in der Aktion der Greenpeaceaktivisten noch keine rechtswidrige Nötigung gesehen habe. Insbesondere aufgrund der geringen Dauer der Blockade, ihrer freiwilligen Beendigung und der Existenz nahegelegener Ausweichmöglichkeiten war die für eine Strafbarkeit erforderliche Zweck-Mittel-Relation und damit ein strafbares Verhalten noch nicht gegeben. Daher bestand insoweit bereits aus Rechtsgründen kein die polizeilichen Speicherungen rechtfertigender Tatverdacht. Ich habe mich deswegen zunächst an die Staatsanwaltschaft gewandt, die meine Auffassung bestätigte. Wie sich herausstellte, hatte die Staatsanwaltschaft bereits zu einem früheren Zeitpunkt das Verfahren wegen Nötigung abgetrennt, da ein Anfangsverdacht wegen Nötigung nicht bejaht wurde. Die Polizei wurde hiervon jedoch nicht in Kenntnis gesetzt.

Die Polizei hat auf meine Aufforderung hin auch die Speicherungen wegen Nötigung aus dem KAN gelöscht.

6.5 Speicherungen im Zusammenhang mit der „Antifa-Passau“

Im Jahre 1998 hatte die Staatsanwaltschaft gegen mehrere mutmaßliche Angehörige der vom Landesamt für Verfassungsschutz als extremistisch eingestuften „Antifa-Passau“ ein Ermittlungsverfahren wegen Bildung einer kriminellen Vereinigung gemäß § 129 Abs. 1 Strafgesetzbuch eingeleitet. Zu diesem Zweck hatte die mit der Ermittlung betraute Polizeidienststelle umfangreiche personenbezogene Daten gespeichert. Das Strafverfahren wurde schließlich von der Staatsanwaltschaft gemäß § 170 Abs. 2 StPO eingestellt. Die o. g. Ermittlungsdatei wurde zunächst gesperrt, nur noch zum Zwecke der Asservatenausgabe geöffnet und anschließend gelöscht.

Unabhängig davon habe ich die Speicherungen zu den vormals Beschuldigten in diesem Zusammenhang überprüft, nachdem mir die Polizei mitgeteilt hatte, dass diese wegen des Verdachts der Bildung einer kriminellen Vereinigung im Kriminalaktennachweis (vgl. Nr. 6.1) gespeichert werden. Für meine Prüfung dieser Speicherungen habe ich exemplarisch einige Ermittlungsakten der ermittlungsführenden Staatsanwaltschaft beigezogen. Daraus ergab sich, dass die Staatsanwaltschaft der Polizei lediglich das Formblatt über die Mitteilung des Verfahrensausgangs ohne die Einstellungsbegründung übersandt hatte. Ein Hinweis der Staatsanwaltschaft, dass der Tatverdacht gegen die Betroffenen entfallen ist, war damit nicht gegeben.

Aufgrund der Einstellungsbegründung der Staatsanwaltschaft und der sonstigen Ermittlungsergebnisse habe ich einen die weitere Speicherung ausreichenden Tatverdacht der Bildung einer kriminellen Vereinigung nicht gesehen.

Die Deliktsbezeichnung „Bildung einer kriminellen Vereinigung“ im Kriminalaktennachweis stellt zudem eine besonders belastende Speicherung dar. Ich habe deshalb die Polizeidienststelle aufgefordert, die Speicherungen im Kriminalaktennachweis zu löschen. Dieser Forderung ist das Landeskriminalamt als speichernde Stelle nachgekommen und hat die Speicherungen gelöscht.

6.6 Speicherungen in sonstigen Dateien

Anlässlich meiner Prüfungen bei bayerischen Polizeidienststellen habe ich neben Speicherungen im Kriminalaktennachweis auch Speicherungen in delikts- und dienststellenspezifischen Dateien überprüft. Im Folgenden sind einige wichtige Feststellungen aus solchen Prüfungen wiedergeben.

Bei einer Polizeidirektion habe ich eine Datei geprüft, die der Unterstützung von Maßnahmen gegen Personen dient, die sich in bestimmten Bereichen der Innenstadt aufhalten und nach Auffassung der Polizei ein Gefahrenpotenzial darstellen. Dabei handelt es sich insbesondere um Personen, die der Rauschgiftszene zugerechnet werden oder die dort lagern, Alkohol trinken, betteln, Passanten anpöbeln, Sitzgelegenheiten der Verkehrsbetriebe besetzen usw. Zur Unterstützung der Maßnahmen, wie Belehrung, Platzverweis, Ordnungswidrigkeitenanzeigen und ggf. strafprozessuelle Maßnahmen, werden diese in der Datei gespeichert.

Ich habe festgestellt, dass bei einigen Speicherungen weder in der Datei selbst, noch in sonstiger Weise nachvollziehbar dokumentiert war, aus welchem Grund eine Speicherung erfolgt ist. Teilweise war nur die Bemerkung „punkerartiges Aussehen“ eingetragen. Ich habe die Polizei darauf hingewiesen, dass ohne Dokumentation der Speicherungsgründe nicht nachvollzogen und geprüft werden kann, ob die nach der Errichtungsanordnung erforderlichen Speicherungsvoraussetzungen vorliegen. Bemerkungen wie „punkerartiges Aussehen“ reichen für eine Speicherung keinesfalls aus. Das äußere Erscheinungsbild allein stellt keinen Speicherungsgrund dar. Ich habe die Polizei deshalb aufgefordert, diese Speicherungen zu überprüfen und bei Fehlen ausrei-

chender Speicherungsgründe zu löschen sowie die Speicherungsgründe für jeden einzelnen Datensatz künftig zu dokumentieren. Die Polizeidirektion hat dies zugesagt und die von mir kritisierten Speicherungen überprüft, gelöscht bzw. korrigiert. Einige Datensätze, deren Speicherungsfrist nach meinen Feststellungen bereits abgelaufen war, wurden gelöscht.

Wie schon im letzten Berichtszeitraum habe ich Speicherungen in der Arbeitsdatei „Rauschgift“ überprüft. Die Datei soll der repressiven und präventiven Bekämpfung der Betäubungsmittelkriminalität einschließlich der Beschaffungs- und Begleitdelinquenz in Bayern dienen.

Bei meiner Prüfung habe ich keine wesentlichen Mängel festgestellt. Einzelne Unzulänglichkeiten konnten bereinigt werden. Beispielsweise wurde eine Person gespeichert, weil in deren Wohnung vier bis fünf Gramm Haschisch und fünf Gramm halluzinogene Pilze aufgefunden wurden. Das Rauschgift konnte keiner der beiden anwesenden Personen zugeordnet werden. Die Staatsanwaltschaft hat das Verfahren deshalb eingestellt. Es lagen auch keine einschlägigen Erkenntnisse über die Betroffenen vor. Der Sachbearbeiter ging deshalb von einem Fall geringerer Bedeutung aus und vergab eine Aussonderungsprüffrist von neun statt zehn Jahren, obwohl für diese Fälle in der Errichtungsanordnung für die Datei bei Erwachsenen eine Verkürzung der Frist bis auf fünf Jahre vorgesehen ist. Die Polizeidienststelle hat die Speicherungsfrist nach erneuter Prüfung auf fünf Jahre verkürzt.

Für problematisch halte ich die mögliche Speicherungsdauer von fünf Jahren für Jugendliche bzw. zehn Jahren für Erwachsene in der Arbeitsdatei „Rauschgift“ als nur „Tatverdächtige“. Nach meinen Feststellungen werden in der Praxis in diesen Fällen kürzere Fristen vergeben. Ich habe deshalb die Polizeidienststelle aufgefordert, die Speicherungsfristen in der Errichtungsanordnung zu verkürzen. Die Polizei hat mir dies zugesagt. Nach meinen Informationen wurde die Neuregelung im Rahmen einer Sachbearbeitertagung für die relevanten Polizeidienststellen bereits umgesetzt. Die Errichtungsanordnung wurde allerdings noch nicht geändert. Die Vorlage wurde mir für die nächste Zeit in Aussicht gestellt.

Geprüft habe ich auch Speicherungen in der Datei für Geldwäsche-Verdachtsanzeigen. Nach § 11 des Geldwäschegesetzes haben u. a. Kredit-, Finanzinstitute und Spielbanken bei Feststellung von Tatsachen, die darauf schließen lassen, dass eine Finanztransaktion einer Geldwäsche dient oder im Fall ihrer Durchführung dienen würde, unverzüglich den Strafverfolgungsbehörden anzuzeigen. Ich habe festgestellt, dass die datenschutzrechtliche Problematik bei den Speiche-

rungen in dieser Datei in der nicht selten relativ geringen Verdachtsschwelle liegt. So konnte mich die Polizei bei einigen Datensätzen von der Zulässigkeit der Speicherungen nur durch die Darlegung weiterer Erkenntnisse überzeugen. In wenigen Fällen, in denen aufgrund meiner Einschätzung die Speicherungsvoraussetzungen nicht erfüllt waren, hat die Polizei die Speicherungen gelöscht oder die Speicherungsfrist verkürzt.

6.7 Meldung und Speicherung extremistischer Gewalttäter

Im Berichtszeitraum war für mich eine Tendenz zur Ausweitung der polizeilichen Datenverarbeitung im Bereich „extremistischer Gewalt“ feststellbar. Ihren Anfang nahm diese Entwicklung mit den Beschlüssen der Innenministerkonferenz am 24.11.2000. Ein Maßnahmenkatalog war als Beitrag zur effektiveren Bekämpfung des Rechtsextremismus beschlossen worden. Auf Initiative Bayerns wurden die ursprünglich nur für diesen Bereich geplanten Maßnahmen auch auf den linksextremistischen Bereich und den Bereich der politisch motivierten Ausländerkriminalität erweitert.

Dazu gehören zum einen die Schaffung bundesweiter Dateien zur Speicherung extremistischer Gewalttäter, sog. Gewalttäterdateien. Darüber hinaus wurden „personengebundene Hinweise“ eingeführt, die extremistische Gewalttäter im bundesweiten Informationssystem der Polizei (INPOL) kennzeichnen sollen. Als weitere Maßnahme wurden die Speicherungskriterien sowie die Meldevoraussetzungen für den kriminalpolizeilichen Meldedienst (KPMD) und die bayerische Staatsschutzdatei (SDBY) erheblich erweitert.

Wegen einer Reihe von Kritikpunkten habe ich mich an das Staatsministerium des Innern gewandt und gemeinsam mit anderen Datenschutzbeauftragten der Länder den Bundesbeauftragten für den Datenschutz in seinen Bemühungen unterstützt, datenschutzrechtliche Verbesserungen zu erzielen:

- Nach den Errichtungsanordnungen für die Gewalttäterdateien können auch „sonstige Personen“ aufgrund präventiv-polizeilicher Maßnahmen, wie der Personalienfeststellung, gespeichert werden, wenn Tatsachen die Annahme rechtfertigen, dass sich die Person künftig an entsprechenden politisch-motivierten Straftaten von erheblicher Bedeutung beteiligen wird.

Es bedarf zumindest der Konkretisierung, welche Tatsachen eine Speicherung rechtfertigen können. Dabei sind an die Prognose hohe Anforderungen zu stellen, die schriftlich begründet werden sollten. Darüber hinaus sollten bei der Speicherung von Daten dieses Personenkreises wesentlich kürzere Speicherungsfristen gelten als beispielsweise für Beschuldigte und Tatverdächtige.

- Die Pflicht zur schriftlichen Dokumentation der Speicherungsgründe muss im Interesse des Betroffenen und der Selbstkontrolle der Polizei auch bei der Speicherung von personengebundenen Hinweisen gelten.

- Eine Speicherung in den bundesweiten Gewalttäterdateien sollte nicht bei jeder politisch motivierten Straftat sondern nur vorgenommen werden, wenn aufgrund der konkreten Umstände von einer Straftat von länderübergreifender oder internationaler Bedeutung auszugehen ist. Eine Prüfung der Bedeutung der Straftat im Einzelfall sollte deshalb in den Errichtungsanordnungen festgelegt werden. Darüber hinaus sollte die Speicherung entsprechend der Bezeichnung der Dateien „Gewalttäter“ - in den Errichtungsanordnungen - auf Gewalttaten von einiger Erheblichkeit beschränkt werden. Dies gilt insbesondere im Hinblick auf die bundesweite Abrufmöglichkeit dieser Daten und der daraus ggf. resultierenden Folgemaßnahmen der Polizei. Auch die Speicherung der personengebundenen Hinweise sollte ausdrücklich an die Voraussetzung „Gewalttätigkeit“ geknüpft werden.

- Für die Speicherung der personengebundenen Hinweise ist eine Speicherungsfrist vorgesehen, die sich nach der Laufzeit der Kriminalakte bzw. der erkennungsdienstlichen Unterlagen richtet. Ich halte es nicht für gerechtfertigt, dass bei Verlängerung der Frist der Kriminalakte die personengebundenen Hinweise auch in den Fällen mitgezogen werden, in denen keine einschlägigen Erkenntnisse hinzugetreten sind. Ich halte es deshalb für erforderlich, für die personengebundenen Hinweise eigenständige Prüffristen vorzusehen.

Auch gegen die Neufassung der Errichtungsanordnung für die Staatsschutzdatei Bayern (SDBY) und die damit verbundenen Modifizierung des kriminalpolizeilichen Meldedienstes (KPMD) habe ich erhebliche datenschutzrechtliche Bedenken geltend gemacht. Die dort vorgesehene Erfassung von Personen bei Straftaten jeglicher Art - soweit ein politisches Motiv zugrundegelegt werden kann - halte ich für zu weitgehend. Ich habe mich entschieden gegen eine mögliche

Speicherung von Personen in einer Staatsschutzdatei gewandt, die in Ausübung ihres Grundrechts der Versammlungsfreiheit im Einzelfall die Grenzen der freien Meinungsäußerung durch einfache Beleidigung überschritten haben. Hierin sehe ich eine Gefahr, dass politisch engagierte Personen als „Staatsgegner“ gespeichert werden.

Ich sehe in der Prüfung von Speicherungen wegen politisch motivierter Straftaten im nächsten Berichtszeitraum einen Schwerpunkt meiner Tätigkeit im Sicherheitsbereich.

6.8 Ausschreibung im geschützten Fahndungsbestand Landfriedensbruch

Der „geschützte Fahndungsbestand Landfriedensbruch und verwandte Straftaten“ dient der Verhütung schwerer Straftaten im Zusammenhang mit politisch bestimmten öffentlichen Versammlungen oder Aufzügen. Der Zugriff auf diese Datei wird nur zu besonderen aktuellen Anlässen auf Anforderung der für den Einsatz zuständigen Polizeidienststelle und mit Zustimmung des Innenministers/Senators des betreffenden Landes für einen festgesetzten Zeit- und Fahndungsraum zur Abfrage freigegeben.

Nachdem der Fahndungsbestand anlässlich des G 8 Gipfeltreffens in Genua im Juli 2001 geöffnet worden war, wurde mehreren darin ausgeschriebenen Personen die Ausreise untersagt.
Bei meiner Prüfung einzelner von bayerischen Polizeidienststellen vorgenommenen Ausschreibungen habe ich festgestellt, dass bei den der jeweiligen Speicherung zu Grunde liegenden Erkenntnissen eine Meldung und damit eine Aufnahme in den geschützten Fahndungsbestand nicht zulässig war.

In einem Fall wurde dem Betroffenen vorgeworfen, während einer Versammlung ein rohes Ei geworfen und damit eine unbekannte Person am Rücken getroffen zu haben. Ich habe das Landeskriminalamt darauf hingewiesen, dass bei diesem Sachverhalt im Gegensatz zur polizeilichen Annahme keine gefährliche Körperverletzung vorliegt, sondern allenfalls der Verdacht einer versuchten Körperverletzung, Beleidigung und Sachbeschädigung besteht. Nach den Richtlinien für den kriminalpolizeilichen Meldedienst „Landfriedensbruch und verwandte Straftaten“ sind zwar Fälle von Straftaten mit Gewalttätigkeiten gegen Leib oder Leben oder gegen fremde Sachen meldepflichtig. Aus Gründen der Verhältnismäßigkeit ist aber auf die Art und Schwere der jeweiligen konkreten Tat abzustellen. Bei geringfügigen Straftaten halte ich daher eine Speiche-

rung angesichts der weit reichenden Folgen für den Betroffenen weder für erforderlich, noch für verhältnismäßig und daher für unzulässig. Im Hinblick darauf, dass in dem dargestellten Fall die angewandte Gewalt sowie auch der ggf. eingetretene Schaden gering und zudem der Verletzungsvorsatz angesichts des angewandten Tatmittels zweifelhaft war, habe ich das Landeskriminalamt aufgefordert, die Speicherung zu löschen. Dem ist das Landeskriminalamt nachgekommen.

Bei einer weiteren Person, die an der Ausreise gehindert wurde, hat meine Prüfung ebenfalls die Unzulässigkeit der Ausschreibung ergeben. Diese Person soll sich bei einer Versammlung wenige Minuten an einer Sitzblockblockade beteiligt haben. Nach der Rechtsprechung des Bundesverfassungsgerichts liegt in diesen Fällen ohne Hinzutreten weiterer Umstände mangels Gewalt keine Nötigung im strafrechtlichen Sinne vor. Anders als von der Polizei angenommen kann dem Betroffenen daher lediglich eine Störung der Versammlung zur Last gelegt werden. Diese Straftat ist aber für den geschützten Fahndungsbestand Landfriedensbruch nicht meldepflichtig. Dort ist zudem ausdrücklich ausgeführt, dass es sich bei Straftaten mit Gewalttätigkeiten um solche mit aggressivem Einsatz physischer Gewalt handeln muss, woran es hier fehlt. Ich habe daher das Landeskriminalamt aufgefordert, auch diese Speicherung zu löschen. Dieser Forderung ist das Landeskriminalamt zwischenzeitlich nachgekommen.

Schließlich habe ich im Rahmen meiner Prüfungen auch festgestellt, dass eine bekannte Persönlichkeit alleine auf Grund von in einem Leserbrief geäußerten Vermutungen im geschützten Fahndungsbestand Landfriedensbruch ausgeschrieben war. Bei einer Großdemonstration mit mehreren Tausend Teilnehmern, bei der auch die bekannte Persönlichkeit teilnahm, kam es unter anderem zu einer Sitzblockade einiger weniger Personen. Nachdem in dem Leserbrief behauptet worden war, auch die bekannte Person habe sich unter den blockierenden Demonstranten befunden, wurde gegen diese ein Ermittlungserfahren eingeleitet. Bei einer späteren Zeugenvernehmung des Verfassers des Artikels stellte dieser klar, dass es sich bei seiner Äußerung lediglich um eine Vermutung gehandelt habe, da er die ihm bekannte Person zu einem späteren Zeitpunkt in der Nähe habe stehen sehen. Obwohl auch vorhandene umfangreiche Videoaufzeichnungen keinen weiteren Tatverdacht ergaben, wurde die bekannte Persönlichkeit dennoch im geschützten Fahndungsbestand Landfriedensbruch ausgeschrieben.

Eine weitere bekannte Persönlichkeit, die ebenfalls bei dieser Demonstration von dem Verfasser des Artikels gesichtet und erwähnt wurde, wurde zwar nicht im geschützten Fahndungsbestand,

wohl aber im Kriminalaktennachweis gespeichert, obwohl auch hier jeglicher Tatverdacht entfallen ist.

Es kann nicht angehen, dass jemand, der zufällig bei einer Demonstration gesehen wird, bei der vorher oder nachher durch Unbekannte eine Straftat begangen wird, gespeichert wird. Ich habe daher das zuständige Polizeipräsidium aufgefordert, sämtliche Speicherung der beiden Persönlichkeiten im Zusammenhang mit der Großdemonstration sowohl im Kriminalaktennachweis als auch im geschützten Fahndungsbestand zu löschen. Dem hat es in vollem Umfang entsprochen.

6.9 Vorratsdatenspeicherung bei Internet- und Telekommunikationsprovidern

Ein Gesetzesentwurf des Bundesrats, der im Bundestag vor der Bundestagswahl nicht mehr beraten wurde, sieht neben anderen Bestimmungen Neuregelungen im Telekommunikations- und im Teledienstedatenschutzgesetz vor, welche die Verpflichtung der Anbieter von Telekommunikations- und Telediensten zur Vorratsspeicherung von Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten ermöglichen sollen. Diese Daten sollen von den Providern für bestimmte Mindestfristen gespeichert werden, damit der Polizei, aber auch dem Verfassungsschutz, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und dem Zollkriminalamt bei evtl. Anlässen eine Nutzung zur Aufgabenerfüllung möglich ist.

Eine solche verdachtslose Speicherung, die rein vorsorglich für den Fall eines späteren Bedarfs durchgeführt wird, ist abzulehnen. Sie stellt eine tiefgreifende Einschränkung des Rechts auf unbeobachtete Telekommunikation dar, die ich für unverhältnismäßig halte, zumal die Daten der weit überwiegend rechtstreuen Bürger nicht benötigt werden. Aufgrund der Sensiblität der Daten, die die Aussagekraft von Inhaltsdaten sogar übertreffen können, solle es bei den bisherigen Zugriffsmöglichkeiten der oben genannten Sicherheitsbehörden bleiben. Eine flächendeckende Speicherung auf Vorrat hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit Nachdruck abgelehnt.

6.10 Errichtungsanordnungen für GAST-Dateien

Auch in diesem Berichtszeitraum wurden mir von Polizeidienststellen wieder zahlreiche Errichtungsanordnungen für sog. GAST-Dateien (Dateien zur Gefahrenabwehr und Verfolgung von

Straftaten und Ordnungswidrigkeiten) vorgelegt. In den Errichtungsanordnungen müssen von der speichernden Stelle u. a. der Zweck der Datei, der betroffene Personenkreis, Art und Umfang der zu speichernden personenbezogenen Daten, die Eingabe- und Zugriffsberechtigungen sowie die Aussonderungsprüffristen festgelegt werden.

Gegen die überwiegende Zahl dieser Errichtungsanordnungen bestanden aus datenschutzrechtlicher Sicht keine Einwände. Bei einzelnen wurden die Speicherungskriterien und -fristen von der Polizei auf meine Forderung hin datenschutzkonform geändert oder ergänzt. Beispielhaft möchte ich auf zwei Errichtungsanordnungen eingehen, die besondere datenschutzrechtliche Probleme aufwiesen:

Ein Polizeipräsidium wollte zur Bekämpfung der Urkundenkriminalität alle in seinem Zuständigkeitsbereich festgestellten Inhaber von Personalausweisen/Pässen von EU-Staaten zum Zwecke der Überprüfung speichern. Zugrunde lagen Erkenntnisse über mehr als 500.000 entwendete Blankopersonalausweise und -reisepässe eines bestimmtes Staats im Jahr 1998, die mit fiktiven oder existenten Personalien ausgefüllt und anschließend zur Einreise in Staaten der EU, zur Beantragung von Aufenthaltserlaubnissen, Arbeitserlaubnissen und Sozialhilfe verwendet werden sollen.

Diese generelle Überprüfung der Ausweise und die dafür vorgesehene Speicherung **aller** EU-Bürger im Zuständigkeitsbereich des Polizeipräsidiums habe ich abgelehnt, da ein Fälschungsverdacht gegen diese Personen insgesamt nicht bestand. Die bloße Möglichkeit einer Fälschung im Einzelfall reicht für eine so weitgehende Maßnahme nicht aus. Erkenntnisse, die für eine Vielzahl gefälschter EU-Ausweise sprechen, hatte das Polizeipräsidium zwar hinsichtlich der Ausweise eines bestimmten EU-Staates genannt, nicht jedoch hinsichtlich der Ausweise **aller** anderen EU-Staaten.

Ich habe deshalb gefordert, die Speicherungsmöglichkeit in der Errichtungsanordnung entsprechend einzuschränken. Das Polizeipräsidium hat mir daraufhin mitgeteilt, dass nur Inhaber von EU-Ausweisen des bestimmten Staates kurzfristig zum Zwecke der Überprüfung gespeichert seien. Die Datei werde wegen des kurz bevorstehenden Abschlusses der Überprüfung gelöscht.

Eine andere Polizeidienststelle hat mir die Errichtungsanordnung für eine Datei zugesandt, deren Zweck es war, aus Sicherheitsgründen Mitarbeiter von Fremd- und Lieferfirmen, die in der Poli-

zeidienststelle tätig werden oder dorthin liefern sollten, zu speichern, nachdem diese mittels Datenabgleich polizeilich überprüft worden waren.

Die Polizeidienststelle hat mir auf Anfrage mitgeteilt, dass die Arbeitgeber der für die Tätigkeit vorgesehenen Mitarbeiter gebeten werden, deren Identitätspapiere in Kopie an die zuständige Verwaltungsdienststelle der Polizei zu senden, damit diese mittels Abgleich mit polizeilichen Informationssystemen auf eine etwaige Sicherheitsgefährdung überprüft werden können. Eine Aufklärung über die Tatsache der Überprüfung oder die Einholung des Einverständnisses des Betroffenen mit der Überprüfung erfolge durch die Polizei nicht. Ob eine Aufklärung oder Befragung der Mitarbeiter durch die Firmen erfolge, sei der Polizei nicht bekannt.

Dieses Verfahren halte ich aus datenschutzrechtlicher Sicht für nicht akzeptabel, da dabei nicht ausgeschlossen werden kann, dass die Daten ohne Kenntnis des Betroffenen erhoben, abgeglichen und gespeichert werden und das Ergebnis der polizeilichen Überprüfung allein dem Arbeitgeber bekannt wird. Dies entspricht nicht dem Unmittelbarkeitsgrundsatz in Art. 30 Abs. 2 Satz 1 Polizeiaufgabengesetz, der vorschreibt, dass die Daten grundsätzlich beim Betroffenen erhoben werden und dem grundsätzlichen Anspruch des Betroffenen zu wissen, was die Polizei über ihn weiß. Eine fachliche Notwendigkeit, diese Maßnahme ohne Kenntnis des Betroffenen durchzuführen, war für mich nicht ersichtlich. Ich habe es deshalb für erforderlich gehalten sicherzustellen, dass die polizeiliche Überprüfung mit freiwilliger, informierter sowie schriftlicher Einwilligung des Arbeitsnehmers erfolgt.

Da ich davon ausgegangen bin, dass diese Überprüfungsmaßnahmen in ähnlicher Weise auch bei anderen Polizeidienststellen durchgeführt werden, habe ich das Innenministerium um Überprüfung des Verfahrens und um Stellungnahme gebeten. Dieses hat mir mitgeteilt, es werde angeordnet, ab sofort durch geeignete Maßnahmen sicherzustellen, dass der Arbeitnehmer von der polizeilichen Überprüfung informiert wird. Damit soll er in die Lage versetzt werden, über die Erteilung oder Nichterteilung seiner Einwilligung zur Datenerhebung, zum Datenabgleich und zur Datenspeicherung zu entscheiden.

6.11 Rasterfahndung

Nach den Terroranschlägen am 11. September 2001 in den USA wurden bundesweit präventivpolizeiliche Rasterfahndungen zur Enttarnung potenzieller Attentäter (sog. Schläfer) durchgeführt. Ausgehend von den Erkenntnissen aus den USA über Persönlichkeitsmerkmale der Täter, die in Deutschland lebten und den Anschlag planten, wurden unter Koordination des Bundeskriminalamts, bestimmte auf den o.g. Personenkreis zutreffende Kriterien erarbeitet. Daraus wurde sodann ein weitgehend bundeseinheitliches Rasterprofil erstellt, mit dessen Hilfe Personen, die über längere Zeit unauffällig in Deutschland leben und Terrorakte planen, erkannt werden sollen. Bei der Rasterfahndung wurden zunächst von verschiedenen Stellen Daten zu Personen angefordert, die dem Täterprofil entsprechen. Diese Datenbestände wurden sodann gegeneinander oder mit anderen polizeilichen oder fremden Datensätzen maschinell abgeglichen. Als Ergebnis der Rastermaßnahme bleiben diejenigen Personen übrig, die alle vorgegebenen Kriterien erfüllen und deshalb einer näheren Überprüfung unterzogen werden. Zu diesen als „Prüffälle“ bezeichneten Personen werden konventionelle polizeiliche Ermittlungen nach den allgemeinen Befugnissen des Polizeiaufgabengesetzes durchgeführt. Sämtliche im Rahmen der Rasterfahndungen übermittelten Daten wurden vom Landeskriminalamt vorübergehend in der Arbeitsdatei „Rasterfahndung BAO-USA“ gespeichert.

Die ermittelten Prüffälle sind zudem in eine weitere Datei „Terror USA“ eingestellt und an das Bundeskriminalamt übermittelt worden. Sie werden dort in einer Verbunddatei vorgehalten.

Rechtsgrundlage für die Rasterfahndung in Bayern ist Art. 44 Polizeiaufgabengesetz (PAG). Danach kann die Polizei von öffentlichen und nicht-öffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien insbesondere Namen, Anschriften, Tag und Ort der Geburt und fahndungsspezifische Suchkriterien zum Zwecke des Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr von Straftaten von erheblicher Bedeutung erforderlich ist. Anders als in zahlreichen anderen Bundesländern wird die Rasterfahndung in Bayern nicht durch ein Gericht angeordnet, sondern durch den Dienststellenleiter mit Zustimmung des Staatsministeriums des Innern. Entsprechend der gesetzlichen Verpflichtung wurde ich unverzüglich unterrichtet, als das Landeskriminalamt im September 2001 die erste Rasterfahndungsanordnung erließ. Seitdem stehe ich in ständigem Kontakt mit dem

Landeskriminalamt und überprüfe laufend die Durchführung der Rasterfahndung. Dabei informiere ich mich über den Stand der Rasterfahndung sowie eventuelle neue Maßnahmen und stelle sicher, dass die gesetzlichen Vorgaben eingehalten werden. Die strikte Beachtung der gesetzlichen Regelungen halte ich gerade bei einer Rasterfahndung für besonders wichtig, da diese Maßnahme eine große Anzahl von völlig Unbeteiligten trifft und es sich selbst bei den Prüffällen in der weit überwiegenden Mehrzahl um Unbeteiligte handelt, die jedoch zahlreichen polizeilichen Maßnahmen ausgesetzt sein können. Daher ist auch besonderer Wert darauf zu legen, dass in die Rechte der Betroffenen nicht mehr als unbedingt erforderlich eingegriffen wird.

Der Umfang der Rasterfahndung und der davon Betroffenen zeigt sich an den Datenerhebungen des Landeskriminalamts. So wurden bei bayerischen Meldebehörden, Ausländerbehörden, Sozialämtern und Universitäten bzw. Hochschulen die Daten sämtlicher Personen angefordert, die folgendem Profil entsprechen:

- männlich
- 18 bis 40 Jahre
- islamische Religionszugehörigkeit
- Meldeanschrift bzw. Wohnort in Bayern
- Student einer Universität bzw. Hochschule mit Schwerpunkt technischer/naturwissenschaftlicher Ausrichtung
- legaler Aufenthaltsstatus
- keine Sozialhilfe
- Geburtsland und/oder Nationalität eines bestimmten Staates (z. B. Afghanistan)

Außerdem trat das Landeskriminalamt mit weiteren Rasterfahndungsanordnungen an die bayerische Industrie- und Handelskammer, die Betreiber kerntechnischer Anlagen und Forschungseinrichtungen in Bayern sowie bayerische Luftämter heran, um sich unter Bezug auf das Täterprofil Inhaber von Gefahrgutscheinen, Besucher bayerischer kerntechnischer Anlagen sowie Inhaber von Luftfahrscheinen und Flugschülern übermitteln zu lassen.

Insgesamt wurden von diesen Stellen ca. 174 000 Daten an das Landeskriminalamt übermittelt. Unter Berücksichtigung von Mehrfachnennungen und nach sonstiger Bereinigung handelte es sich um Personendatensätze zu ca. 94 000 Personen, die in die Rasterfahndung einbezogen wurden. Nach Durchführung der maschinellen Abgleiche blieben schließlich ca. 1900 Prüffälle üb-

rig, die derzeit durch die Kriminalpolizeidienststellen näher überprüft werden. Die Abarbeitung der Prüffälle ist noch nicht abgeschlossen, sie wird noch einige Zeit in Anspruch nehmen. Sobald sich bei der Bearbeitung herausstellt, dass eine erfasste Person nicht dem Grundraster unterfällt wird sie nach Auskunft des Landeskriminalamts ausgeschieden und in der Datei „Rasterfahndung BAO-USA“ gelöscht. Dies habe ich an Hand von Stichproben überprüft und - abgesehen von Einzelfällen - die Richtigkeit der Auskunft festgestellt.

In der Presse wurde immer wieder über Urteile von Gerichten berichtet, die die Rasterfahndung in anderen Bundesländer für rechtswidrig erklärt haben. Diese Entscheidungen habe ich daraufhin überprüft, ob sich aus den jeweiligen Begründungen Rückschlüsse auf die Rechtmäßigkeit der Rasterfahndung in Bayern ergeben könnten. Dies war jedoch nicht der Fall, da die gesetzlichen Regelungen in den Ländern unterschiedlich sind. Im Gegensatz zu den landesrechtlichen Vorschriften der Länder, in denen entsprechende Urteile erlassen wurden, verlangt das Bayerische Polizeiaufgabengesetz nämlich nicht das Vorliegen einer gegenwärtigen Gefahr.

Auch in Bayern verlief die Rasterfahndung nicht immer reibungslos. So enthielten die ersten Rasterfahndungsanordnungen das Kriterium des Sozialhilfebezugs als ausschließendes Merkmal, obwohl nach den damals geltenden Vorschriften des Sozialgesetzbuchs eine Datenübermittlung an Polizeibehörden für die Zwecke einer Rasterfahndung nicht zulässig war. Nachdem ich das Landeskriminalamt auf diese Rechtslage hingewiesen hatte, habe ich in Zusammenarbeit mit dem Landeskriminalamt, dem Innenministerium und dem Ministerium für Arbeit und Sozialordnung, Familie und Frauen ein Verfahren erarbeitet, das dennoch einen datenschutzkonformen Abgleich mit Sozialdaten zuließ. Um dies zu erreichen, musste sichergestellt werden, dass das Landeskriminalamt vom Inhalt der Sozialdaten keine Kenntnis erhält. Hierzu wurde ein sogenanntes Black-Box-Verfahren eingesetzt, bei dem die Anstalt für Kommunale Datenverarbeitung Bayern (AKDB) im Auftrag der jeweiligen Gemeinden den Abgleich zwischen dem zur Rasterfahndung erhobenen Datenbestand der Polizei und dem Bestand der Sozialhilfeempfänger vornahm. Der so erzeugte Datenbestand durfte nur zum Abgleich mit dem von den Universitäten und Hochschulen übermittelten Datenbestand verwendet und musste sodann als gesperrte Datei verwahrt werden. Ferner sicherte das Landeskriminalamt zu, dass auch keine sonstige Rekonstruktion der Sozialhilfeempfänger durch Abgleich der verfügbaren Datenbestände erfolgt. Durch diese Verfahrensweise war sichergestellt, dass das Landeskriminalamt keine Kenntnis davon erhält, welche Personen Sozialhilfe beziehen.

Zwischenzeitlich wurde das Sozialgesetzbuch durch das Terrorismusbekämpfungsgesetz dergestalt geändert, dass nunmehr bestimmte Sozialdaten auch zu Zwecken der Rasterfahndung an die Polizei übermittelt werden dürfen. Das angewandte Black-Box-Verfahren wäre daher nach heutiger Rechtslage nicht mehr erforderlich.

Im Januar 2002 wurden sowohl die Daten der Sozialhilfeempfänger bei der Anstalt für Kommunale Datenverarbeitung Bayern als auch die beim Landeskriminalamt unter Verschluss gehaltene Ergebnismenge des Abgleichs der Sozialdaten mit den polizeilichen Daten vernichtet, da die Datenbestände nicht mehr benötigt werden.

Besonderes Augenmerk habe ich auf die möglichst frühzeitige Löschung nicht mehr benötigter Daten gerichtet. Nach Art. 44 Abs. 3 PAG sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Unterlagen, soweit sie nicht zur Verfolgung von Straftaten erforderlich sind, unverzüglich zu vernichten, sobald der Zweck der Maßnahme erreicht ist.

Obwohl jedoch der Datenabgleich und damit die Rastermaßnahmen nach Auffassung des Landeskriminalamts zwischenzeitlich abgeschlossen sind, hat das Landeskriminalamt die Datei „Rasterfahndung BAO-USA“, in der sämtliche angefallenen Daten gespeichert sind, noch nicht gelöscht sondern lediglich gesperrt. Ebenso wie das Innenministerium vertritt es die Auffassung, dies sei erforderlich, da nicht auszuschließen sei, dass sie für eine neu angeordnete Rasterfahndung wieder benötigt werden. Meiner Ansicht nach widerspricht eine solche vorsorgliche Vorratsdatenspeicherung der gesetzlichen Regelung. Da der Zweck der Maßnahme, für den die Daten erhoben wurden erreicht ist, sind die nicht mehr erforderlichen Daten unverzüglich zu löschen. Zweck der Maßnahme ist die Durchführung des Abgleichs mit den in den Rasterfahndungsanordnungen aufgeführten Daten zur Ermittlung von Trefferfällen. Diese stehen nach Angaben des Landeskriminalamts bereits fest und können abgearbeitet werden. Ich habe daher das Landeskriminalamt aufgefordert, die Arbeitsdatei „Rasterfahndung BAO-USA“ sowie die entsprechenden Unterlagen unverzüglich zu löschen, soweit sie nicht zur Verfolgung von Straftaten erforderlich sind. Das Landeskriminalamt hat dies mit der Begründung abgelehnt, der Zweck der Rasterfahndung sei noch nicht erreicht, da die Prüffälle noch nicht vollständig abgearbeitet seien. Auch wenn derzeit keine Notwendigkeit gesehen werde, auf die Daten zuzugreifen, sei die Maßnahme insgesamt noch nicht beendet. Ein Zugriff müsse aber bis zum Abschluss der Maßnahmen gewährleistet werden. Das Innenministerium, das die Auffassung des Landeskriminalamts

teilt, hat dementsprechend der weiteren Aufbewahrung der Daten bis zum Abschluss der Rastermaßnahmen befristet zugestimmt.

Ich halte diese Ansicht aus den o.g. Gründen nicht für zutreffend und werde deshalb eine Beanstandung prüfen.

6.12 DNA-Analyse zu Strafverfolgungszwecken

6.12.1 Beschluss des Bundesverfassungsgerichts vom 14.12.2000

Am 14.12.2000 hat das Bundesverfassungsgericht in einem Beschluss (NJW 2001, Seite 879 ff) über die gesetzlichen Grundlagen für eine richterlich angeordnete Entnahme von Körperzellen und deren molekulargenetische Untersuchung zur Identitätsfeststellung in künftigen Strafverfahren entschieden und diese für verfassungsgemäß befunden. In diesem Beschluss, der durch ein Urteil vom 15.03.2001 (NJW 2001, Seite 2320 ff) ergänzt und fortgeführt wurde, hat das Bundesverfassungsgericht in sehr detaillierter Form Vorgaben für die Anwendung und Auslegung der gesetzlichen Grundlagen für eine DNA-Analyse zu Strafverfolgungszwecken gemacht. Hierbei hat es hervorgehoben, dass nach der gesetzlichen Regelung eine molekulargenetische Untersuchung nur angeordnet werden darf, wenn bei dem Betroffenen eine Straftat von erheblicher Bedeutung vorliegt. Dies ist nach der gerichtlichen Definition eine Straftat, die mindestens dem Bereich der mittleren Kriminalität zuzurechnen ist, den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Erfüllt eine Tat eines der vom Gesetzgeber aufgeführten Regelbeispiele, so ist damit nicht automatisch eine Straftat von erheblicher Bedeutung gegeben. Jede Tat muss im Einzelfall auf ihr Gewicht und ihre Bedeutung für Rechtsfrieden und Sicherheitsgefühl hin überprüft werden. Die Entscheidung über das Vorliegen einer Anlasstat sowie über die Annahme, dass auch künftig gegen den Betroffenen Strafverfahren wegen einer derartigen Straftat zu führen sind, setzt dabei voraus, dass ihr eine zureichende Sachaufklärung insbesondere durch Beiziehung der verfügbaren Straf- und Vollstreckungsakten, des Bewährungsheftes und zeitnaher Auskünfte aus dem Bundeszentralregister vorausgegangen ist und in den Entscheidungsgründen die bedeutsamen Umstände abgewogen werden. Gegebenenfalls ist sogar eine zusätzliche Beweiserhebung, etwa durch die Einholung ärztlicher Aufklärung oder Einsichtsnahme in den Betreuungsakt zu betreiben. Schließlich müssen die Tatsachen, auf denen die Entscheidung beruht, nachvollziehbar dokumentiert werden.

In Reaktion auf diese Rechtsprechung hat das Staatsministerium des Innern die Dienststellen der Bayerischen Polizei auf den Beschluss des Bundesverfassungsgerichtes hingewiesen und für die erforderliche Dokumentation bezüglich Anlasstat und Prognose künftiger Strafverfahren die Verwendung eines einheitlichen Formblattes angeordnet. Allerdings musste ich anlässlich einer Prüfung der praktischen Umsetzung des DNA- Identitätsfeststellungsgesetzes bei einer Polizeidirektion feststellen, dass dort neben einem Auszug aus der Datei Kriminalaktennachweis (KAN) sowie dem Bundeszentralregister in sämtlichen Fällen lediglich die bei der durchführenden Dienststelle vorliegenden eigenen Kriminalakten zur Aufklärung des Sachverhaltes beigezogen wurden. So wurden bspw. bei einem Betroffenen nur die polizeilichen Akten zu zwei Verurteilungen herangezogen, die Einbruchsdiebstähle in ein Vereinsheim bzw. mehrere Bauwägen betrafen, die der Betroffene als Heranwachsender sämtlich innerhalb eines Zeitraumes von 1 Woche und in betrunkenem Zustand begangen hatte. Unterlagen zu einer weiteren, zeitlich nachfolgenden Verurteilung, ebenfalls wegen schweren Diebstahls, wurden nicht beigezogen, da die Kriminalakten hierzu nicht bei der durchführenden Dienststelle geführt wurden. Da aber gerade bei einem heranwachsenden Täter bei Taten innerhalb eines zeitlich eng begrenzten Rahmens besondere Faktoren mit Ausnahmecharakter für dessen Straffälligkeit verantwortlich sein können, hätten Unterlagen über sein weiteres Auftreten zur Beurteilung, ob weitere Strafverfahren gegen ihn zu befürchten sind, herangezogen werden müssen. Auf meine Intervention, auch gegenüber dem Staatsministerium des Innern, hat sich die betreffende Dienststelle zwischenzeitlich bereit erklärt, zur Überprüfung ihrer Prognose auch die Strafakten zu der nachfolgenden Verurteilung beizuziehen, um die weitere Entwicklung des Betroffenen zu berücksichtigen. In diesem Zusammenhang habe ich gegenüber dem Staatsministerium des Innern auch darauf hingewiesen, dass die Beiziehung lediglich der bei der Polizei geführten Kriminalakten nicht dem vom Bundesverfassungsgericht geforderten Gebot bestmöglicher Sachaufklärung entspricht, da die vom Gericht hierzu beispielhaft aufgeführten Unterlagen zur Überprüfung der Prognose in der Regel zusätzliche Erkenntnisse, etwa über Begutachtungen oder die weitere Führung des Betroffenen nach der Verurteilung, enthalten, die im Kriminalakt nicht erfasst sind. Das Innenministerium hat mir hierzu mitgeteilt, dass im Einzelfall, sofern die polizeiliche Akte kein ausreichendes Material für eine ausgewogene Prognoseentscheidung beinhaltet, die Möglichkeit der zusätzlichen Anforderung von Justizakten besteht.

Anlässlich meiner Rechtsprüfung habe ich aber auch festgestellt, dass der Begriff der Straftat von erheblicher Bedeutung als Anlasstat für eine DNA-Analyse bisweilen sehr schematisch und

nicht im Sinne der vom Bundesverfassungsgericht geforderten Einzelfallprüfung angewendet wurde. Als problematisch erwies sich hierbei insbesondere die im Gesetz genannte Katalogtat eines Diebstahls im besonders schweren Fall. Gerade bei diesen Delikten besteht ein besonderes Bedürfnis, zu prüfen, ob die konkrete Tat wegen ihres Gewichtes und Ihren Auswirkungen auf den Rechtsfrieden sowie das Gefühl der Rechtssicherheit der Bevölkerung als eine Tat von erheblicher Bedeutung einzustufen ist. Dass dem nicht in jedem Fall Rechnung getragen wurde, konnte ich bei einem Vorgang feststellen, in dem ein 7 Jahre zurückliegender Diebstahl eines abgesperrten Fahrrades im Wert von 490,-DM zum Anlass für eine DNA-Analyse genommen wurde. Auch meine Korrespondenz mit dem Staatsministerium des Innern konnte bislang keine andere Beurteilung des Falles bewirken.

6.12.2 Formblatt für die Einwilligung in eine DNA-Analyse

Bei der Durchführung von DNA-Analysen zu Strafverfolgungszwecken sowie bei den hierfür erforderlichen Probenentnahmen hat die Polizei in Bayern von Anfang an versucht, diese auf Grundlage einer Einwilligung der Betroffenen, ohne richterlichen Beschluss durchzuführen (siehe zu meinen grundsätzlichen Bedenken gegen die „Einwilligungslösung“ 19. Tätigkeitsbericht Nr. 7.2.3.1). Zur Einholung einer solchen Einverständniserklärung verwendete sie bisher zwei Formblätter, in denen die Betroffenen zur Speichelabgabe vorgeladen wurden bzw. ihr Einverständnis mit der Maßnahme erklären sollten. Auch wenn ich weiterhin Bedenken gegen die Durchführung molekulargenetischer Untersuchungen auf der Grundlage einer Einverständniserklärung der Betroffenen habe, habe ich dennoch gegenüber dem Staatsministerium des Innern die Berücksichtigung datenschutzrechtlicher Mindestanforderungen bei der praktischen Umsetzung gefordert. Besonders wichtig war mir hierbei, dass die mit dem Formblatt verbundenen Hinweise über Voraussetzungen und Folgen einer Einverständniserklärung den Betroffenen so frühzeitig zugesandt werden, dass diesen ausreichend Zeit für eine ausgewogene Entscheidung und ggf. die Beratung mit einer Vertrauensperson bleibt. Weiterhin sollten die Betroffenen in dem Formblatt über die voraussichtliche Speicherungsdauer der aus der DNA-Analyse gewonnenen Daten sowie über die Möglichkeit, ihr einmal erteiltes Einverständnis zu widerrufen, aufgeklärt werden. Schließlich habe ich die Bezeichnung des zur Terminsbestimmung versandten Formblattes als „Vorladung“ kritisiert, da hierdurch der unzutreffende Eindruck entstehen könnte, es bestehe eine Pflicht, zu der Speichelabgabe zu erscheinen.

Das Staatsministerium des Innern war zunächst in keinem dieser Punkte bereit, meinen Forderungen zu entsprechen, hat dies im weiteren aber revidiert.

In seiner Entscheidung vom Dezember 2000 hat das Bundesverfassungsgericht festgestellt, dass das Interesse der Betroffenen an einem effektiven Grundrechtsschutz durch den gesetzlich vorgeschriebenen Richtervorbehalt berücksichtigt wird. Vor dem Hintergrund dieses deutlichen Hinweises auf die absolute Bedeutung des Richtervorbehaltes, die eine Ersetzung des gesetzlichen Schutzsystems durch die Einwilligung als höchst problematisch erscheinen lässt, habe ich gegenüber dem Staatsministerium des Innern erneut auf meine Forderungen rekurriert und verlangt, die Betroffenen in einprägsamer Weise darüber aufzuklären, dass sie mit der Erteilung ihrer Einwilligung auf den gesetzlichen Schutzmechanismus der richterlichen Prüfung, Prognose und Entscheidung verzichten.

Diesen Hinweis hat das Ministerium bei der Gestaltung seiner Formblätter übernommen. Zur Frage einer frühzeitigen Aufklärung der Betroffenen konnte ich erreichen, dass nunmehr auch Gefangene zunächst über die vorgesehenen Maßnahmen und ihre Rechtsfolgen schriftlich belehrt werden, bevor ein Polizeibeamter sie zur Erteilung ihres Einverständnisses mit der Abgabe einer Speichelprobe und deren molekulargenetischer Analyse aufsucht. Tatsächlich waren bisher Strafgefangene nicht vorab von dem Termin zur Speichelentnahme informiert worden und sollten die Abgabe ihrer Einwilligung unmittelbar beim ersten Besuch des Polizeibeamten entscheiden.

Zur Einführung einer Belehrung über die Fristen, nach denen die Speicherung der gewonnenen Daten in der DNA-Analyse-Datei zu prüfen ist, sowie über die Möglichkeit, eine einmal erklärte Einwilligung zu widerrufen, ist das Staatsministerium des Innern jedoch weiterhin nicht bereit. Immerhin soll das Anschreiben an die Betroffenen, in dem die Termine zur Entnahme einer Speichelprobe vorgeschlagen werden, nun nicht mehr als „Vorladung“ bezeichnet werden.

Angesichts der trotz der Lücken doch weitgehenden Aufnahme meiner Vorschläge zur Verbesserung der Information des Einwilligenden habe ich ungeachtet meiner grundsätzlichen Vorbehalte gegen das praktizierte Verfahren von einer Beanstandung abgesehen. Seit Juni 2002 finden die neuen Formblätter bei allen Dienststellen der Bayerischen Polizei Verwendung.

6.12.3 Einwilligungserklärung im Maßregelvollzug

Für im Maßregelvollzug befindliche Personen konnten meine Vorbehalte jedoch nicht behoben werden. Die Unterbringung in einer Anstalt des Maßregelvollzuges wird durch das Gericht insbesondere angeordnet, wenn jemand eine Tat im Zustand der Schuldunfähigkeit oder der verminderten Schuldfähigkeit begangen hat und eine Gesamtwürdigung ergibt, dass von ihm infolge seines Zustandes erhebliche rechtswidrige Taten zu erwarten sind und er deshalb für die Allgemeinheit gefährlich ist. Die Einholung eines Einverständnisses des Betroffenen zur Durchführung einer DNA-Analyse ist bei diesen Personen bereits deswegen problematisch, weil sie sich aufgrund ihrer Unterbringung in einer besonderen Zwangssituation befinden und von einer Einwilligung Vergünstigungen oder von deren Ablehnung Nachteile im Vollzug erwarten könnten. Die Unterbringung im Maßregelvollzug setzt aber zusätzlich eine Störung der geistigen Gesundheit voraus, aufgrund derer erhebliche Zweifel an der Fähigkeit der Untergebrachten zur Willensbildung sowie zur Abschätzung möglicher Folgen ihrer Entscheidung bestehen. Bei diesem Personenkreis komme eine Einverständniserklärung überhaupt nur dann als Grundlage intensiver Grundrechtseingriffe, wie der DNA-Analyse und Speicherung in Frage, wenn Zweifel an der Autonomie der Entscheidung definitiv ausgeschlossen sind.

Vor diesem Hintergrund habe ich die Durchführung der DNA-Analyse aufgrund Einwilligung der Betroffenen im Maßregelvollzug bei einer Polizeidirektion überprüft. Hierbei habe ich in mehreren Fällen festgestellt, dass selbst bei aus dem Kriminalakt ersichtlichen Umständen, die Anlass für Zweifel an der Entscheidungs- und Steuerungsfähigkeit geben mussten, eine weitere Aufklärung unterblieb und dennoch eine Einwilligung des Betroffenen eingeholt wurde, aufgrund derer dann die DNA-Analyse durchgeführt wurde. Am offenkundigsten war dies bei einem Betroffenen der Fall, den der polizeiliche Sachbearbeiter im Ermittlungsverfahren als geistig weit zurückgeblieben eingeschätzt hatte und über den im Kriminalakt vermerkt war, dass er unter anderem wegen seiner Intelligenzminderung als zu 80 % schwerbehindert gilt. Obwohl zudem seine Vernehmung im Ermittlungsverfahren nur mit Dolmetscher durchgeführt werden konnte, wurde (ohne Dolmetscher) eine Einverständniserklärung von ihm erholt und diese zur Grundlage für eine DNA-Analyse gemacht. In ihrer Stellungnahme zu diesem und weiteren von mir aufgezeigten Fällen führte die Polizei hierzu aus, dass sich für die jeweiligen Sachbearbeiter zum Zeitpunkt ihrer Maßnahme keine Zweifel an der Einwilligungsfähigkeit ergeben hätten. In

einem Fall wurde das sogar damit begründet, dass sich weitere Unterlagen, wie ein psychiatrisches Gutachten oder eine Urteilsbegründung nicht im Kriminalakt befunden hätten.

Bei Eingriffen einer Behörde in die Grundrechte eines Bürgers trifft aber diese die Pflicht, das Vorliegen einer hierzu erforderlichen Ermächtigungsgrundlage, in diesem Fall einer wirksamen Einwilligung, zu prüfen und, gegebenenfalls durch Einholung weiterer Informationen, zu belegen. Bei im Maßregelvollzug untergebrachten Personen ergeben sich bereits aus ihrer Unterbringung, die eine Störung der geistigen Gesundheit voraussetzt, Zweifel an deren Einsichts- und Steuerungsfähigkeit. Gerade bei pathologischen Störungen kann auch der unmittelbare Kontakt des polizeilichen Sachbearbeiters mit dem Betroffenen anlässlich der Einholung der Einverständniserklärung diesem als medizinischem Laien keine sicheren Erkenntnisse über die Fähigkeit des Betroffenen zur verantwortlichen Entscheidungsfindung vermitteln. Ausschlaggebend für die Frage, ob eine Einwilligung wirksam ist und somit Grundlage für einen Grundrechtseingriff sein kann, ist daher nicht die persönliche Einschätzung des jeweiligen Sachbearbeiters sondern die objektive Lage. Fortbestehende Zweifel müssen aber letztlich immer zur Herbeiführung einer richterlichen Entscheidung führen. Ich habe mich daher an das Staatsministerium des Innern gewandt und gefordert, bei im Maßregelvollzug untergebrachten Personen DNA-Analysen zu Strafverfolgungszwecken nur noch aufgrund richterlicher Anordnung durchzuführen, andernfalls habe ich eine Beanstandung angedroht.

Das Innenministerium hat daraufhin angeordnet, dass in diesen Fällen regelmäßig eine richterliche Anordnung einzuholen sei, soweit Zweifel an der Einsichtsfähigkeit bestünden. Eine DNA-Maßnahme bei im Maßregelvollzug untergebrachten Personen auf freiwilliger Basis sei nur denkbar, wenn "eine einwilligungsbezogene ausreichende ärztliche Begutachtung" vorausginge und diese entsprechend dokumentiert werde. Diese Anordnung stellt zwar eine nicht unwesentliche Verbesserung dar, der sauberste Weg wäre für mich gleichwohl, im Maßregelvollzug immer eine richterliche Entscheidung einzuholen. In den von mir festgestellten Fällen, in denen Anhaltspunkte für eine ausgeschlossene oder verminderte Einsichtsfähigkeit vorliegen, wird eine richterliche Anordnung nachgeholt oder die Speicherung in der DNA-Analysedatei des Bundeskriminalamtes gelöscht werden müssen. Andernfalls werde ich, wie angekündigt, eine Beanstandung prüfen.

6.12.4 Einwilligungserklärung bei vorläufig Festgenommenen

Ein weiteres problematisches Vorgehen bei der Einholung von Einwilligungen für die DNA-Analyse musste ich anlässlich der Prüfung einer Polizeidienststelle feststellen. Nach meinen Feststellungen wird bei Beschuldigten, die sich nach ihrer Ergreifung im polizeilichen Gewahrsam befinden, die Entnahme der Speichelprobe zum Zwecke der DNA-Analyse und präventiven Speicherung im Rahmen der erkennungsdienstlichen Behandlung und die Belehrung sowie die Abnahme der vorherigen Einwilligungsklärung **im Rahmen seiner Vernehmung** durchgeführt. Ein solcher Betroffener steht durch seine Festnahme im Zusammenhang mit einer Straftat sowie durch die Vernehmungssituation unter einer großen psychischen Belastung. In einer derartigen Lage kann in der Regel von einer wirksamen Einwilligung mit der Durchführung einer DNA-Analyse zur zukünftigen Strafverfolgung nicht ausgegangen werden. Ich habe die betreffende Polizeidienststelle deshalb aufgefordert, diese Praxis zu beenden. Die Dienststelle hat eine Änderung ihrer bisherigen Vorgehensweise jedoch abgelehnt, da ein späteres Aufsuchen des Betroffenen in der Untersuchungshaft zu aufwändig sei bzw. sich der Betroffene bei Entlassung aus dem polizeilichen Gewahrsam der Maßnahme entziehen könnte.

In einem erneuten Schreiben an die Polizei habe ich darauf hingewiesen, dass die Analyse und Speicherung eines DNA-Musters einen erheblichen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt, zu dessen Schutz die Maßnahme unter den Vorbehalt einer richterlichen Entscheidung gestellt wurde. Eine Einwilligung des Betroffenen, die die richterliche Entscheidung ersetzen soll, kann, ungeachtet meiner generellen Einwände hiergegen, nur dann eine ausreichende Rechtsgrundlage für den Eingriff darstellen, wenn sie freiwillig und informiert erfolgt. Die besondere Situation aufgrund von Festnahme, Beschuldigtenvernehmung und weiteren repressiven Maßnahmen wird für eine klare, unbeeinflusste Entscheidung in vielen Fällen keinen Raum lassen. Eine solche Einwilligung, noch dazu wenn sie unter Zeitdruck abgegeben wird, halte ich regelmäßig für unwirksam. Ich habe daher die Polizeidienststelle nochmals aufgefordert, ihr bisher praktiziertes Verfahren nicht weiter fortzusetzen. Andernfalls werde ich - wie angekündigt - eine Beanstandung prüfen.

6.13 Videoüberwachung öffentlicher Straßen und Plätze

In meinem letzten Tätigkeitsbericht (Nr. 5.6.4) hatte ich darauf hingewiesen, dass ich die Schaffung einer gesetzlichen Regelung der Voraussetzungen einer Videoüberwachung öffentlicher Straßen und Plätze für dringend notwendig erachte. Zwischenzeitlich wurde das Polizeiaufgabengesetz um eine ausdrückliche Regelung zur polizeilichen Videoüberwachung ergänzt.

Nach Art. 32 Abs. 2 PAG neue Fassung kann die Polizei zur Abwehr einer im Einzelfall bestehenden Gefahr an öffentlich zugänglichen sog. verrufenen Orten sowie an öffentlich zugänglichen Orten, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden, offen Bild- und Tonaufnahmen oder -aufzeichnungen von Personen anfertigen.

Ich hatte stets betont, dass ich eine flächendeckende Beobachtung aus verfassungsrechtlichen Gründen für unzulässig halte, weil der davon ausgehende ständige Anpassungsdruck die freie Entfaltungsmöglichkeit des Menschen beeinträchtigt. Bezugnehmend auf von mir geäußerte Befürchtungen im Hinblick auf den im Zusammenhang mit den Vollzugshinweisen insoweit nicht eindeutigen Regelungsgehalt hat das Staatsministerium des Innern versichert, dass die gesetzliche Regelung nur kriminalitätsbelastete Orte (so genannte Kriminalitätsschwerpunkte) erfasse.

Zwischenzeitlich wurden auf der Grundlage dieser neuen Vorschrift in zwei Städten Kameras neu aufgebracht. So hat die Polizei eine Videoüberwachung auf dem Münchner Oktoberfest durchgeführt. Dabei wurden neun Kameras über das Gelände verteilt, um bei evtl. Vorkommnissen schneller und gezielter reagieren zu können. In der Videozentrale der Wiesn-Wache verfolgten ständig zwei Polizeibeamte auf den Bildschirmen das Geschehen, so dass bei Bedarf sofort Einsatzkräfte an einen Krisenpunkt entsandt werden konnten. Zusätzlich wurde das gesamte Geschehen auf Videobändern aufgezeichnet, was bei evtl. Strafanzeigen zu einem späteren Zeitpunkt der Aufklärung von Straftaten dienen sollte.

Die Münchner Polizei hat mich frühzeitig über die geplante Videoüberwachung unterrichtet. Außerdem habe ich mich auch direkt vor Ort über die Kamerastandorte und das gesamte Verfahren der Videoüberwachung informiert. Bei meiner Prüfung bin ich zu dem Ergebnis gelangt, dass

aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken gegen die Anfertigung von Bildaufzeichnungen auf der Wiesn bestehen. Nach Art. 32 Abs. 2 Nr. 2 Polizeiaufgabengesetz (PAG) kann die Polizei an öffentlich zugänglichen Orten, von denen auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass dort Personen Straftaten verabreden, vorbereiten oder verüben, offen Bild- und Tonaufzeichnungen von Personen anfertigen. Aus den mir vorliegenden Kriminalitätszahlen für die Wiesn 2000 und 2001 sind jeweils Hunderte von Straftaten ersichtlich, so dass von einem solchen Ort im Sinne des Gesetzes ausgegangen werden kann.

Ich hatte die Polizei jedoch rechtzeitig darauf hingewiesen, dass nach Art. 32 Abs. 2 Satz 2 PAG in geeigneter Weise auf die Bildaufnahmen und -aufzeichnungen hingewiesen werden soll. Das Polizeipräsidium München vertrat in einem Schreiben kurz vor Beginn der Wiesn die Auffassung, der gesetzlichen Hinweispflicht sei durch offensive Öffentlichkeitsarbeit Genüge getan. Demgegenüber habe ich einzelne Berichte über die Videoüberwachung in den Medien nicht als ausreichende Hinweise angesehen. Zum einen kann schon nicht davon ausgegangen werden, dass die aus Deutschland kommenden Besucher der Wiesn in ihrer Gesamtheit die Gelegenheit hatten, diese Berichte zu lesen. Zum anderen handelt es sich bei der Wiesn um ein Volksfest, zu dem eine Vielzahl internationaler Besucher aus der ganzen Welt anreisen. Es muss daher angenommen werden, dass ein großer Teil dieser Wiesnbesucher aus örtlichen und sprachlichen Gründen überhaupt nicht in der Lage ist, die Zeitungsberichte zu lesen und sich auf diesem Wege über die Videoüberwachung zu informieren. Ich habe deshalb vorgeschlagen, Hinweisschilder an den Eingängen zur Wiesn und am U-Bahn-Aufgang anzubringen, die das Polizeipräsidium München als Veranlasser der Videoüberwachung erkennen lassen und die im Hinblick auf die internationalen Besucher der Wiesn auch in englicher Sprache abgefasst sowie mit der grafischen Darstellung einer Kamera versehen sind.

Dem ist das Polizeipräsidium München - wenn auch wegen des Zeitablaufs erst einige Trage nach Wiesenbeginn - nachgekommen.

Die Nürnberger Polizei führt in der Innenstadt eine Videoüberwachung durch. In einem vom Staatsministerium des Innern initiierten dreimonatigen Pilotversuch soll dabei erstmals eine neuartige, nicht leitungsgebundene Videoüberwachungsanlage erprobt werden. Hierfür wurden zwei Kameras installiert, die permanent aufzeichnen. Nach sieben Tagen werden die Aufzeichnungen automatisch überschrieben. In der Umgebung der Kameras wurden mehrere Schilder, die auf die Videoüberwachung hinweisen, angebracht.

Zur Auswahl der nunmehr überwachten Örtlichkeiten wurde mitgeteilt, eine über den Zeitraum von ca. 3 ½ Jahren vorgenommene Auswertung des Lagebilds habe im Vergleich zum übrigen Stadtgebiet eine erhöhte Belastung mit Straftaten, Ordnungswidrigkeiten und Sicherheitsstörungen ergeben. Zur Überprüfung der gesetzlichen Voraussetzungen für die Videoüberwachung habe ich mir die Kriminalitätszahlen für die betreffenden Bereiche vorlegen lassen. Während sich aus den genannten Sicherheitsstörungen und den pauschal aufgeführten Ordnungswidrigkeiten keine eindeutigen Schlüsse ziehen lassen, sprechen die zahlreichen registrierten Straftaten dafür, dass es sich um besonders kriminalitätsbelastete Orte handelt, an denen nach Art. 32 Abs. 2 Nr. 2 PAG eine Videoüberwachung statthaft ist.

Die Besonderheit des Pilotversuchs liegt darin, dass es sich erstmals um nicht kabelgebundene Kameras handelt, die nach Angaben des Innenministeriums in kürzester Zeit auf- und abgebaut und damit an die jeweiligen polizeilichen Brennpunkte versetzt werden können. Ich hatte daher die Gefahr gesehen, diese Mobilität könne dazu verführen, dass die gesetzlichen Voraussetzungen für den Einsatz der Kameras am jeweiligen Ort nicht genau genug geprüft werden. Daher habe ich mich bei einem Informationsgespräch in Nürnberg über die weiteren Planungen erkundigt und die Kameras vor Ort besichtigt. Dabei wurde mir zugesichert, dass die gesetzlichen Voraussetzungen vor einem Wechsel des Kamerastandorts gewissenhaft geprüft werden und ich über jeden Standortwechsel der Videokameras unverzüglich in Kenntnis gesetzt werde. Außerdem sei ein kurzfristiger und ständig wechselnder Einsatz der Kameras derzeit nicht geplant.

Auch das Polizeipräsidium Regensburg führte ein Pilotprojekt zur polizeilichen Videoüberwachung durch, das bereits abgeschlossen ist. Ich habe das Polizeipräsidium Regensburg nunmehr aufgefordert, mir die Erkenntnisse über die Auswirkungen der Videoüberwachung mitzuteilen. Eine solche Evaluierung der Maßnahme durch Auswertung der Kriminalitätszahlen für die Überwachungsgebiete sowie evtl. sonstiger Erkenntnisse (z.B. zur Kriminalitätsverlagerung) halte ich für die datenschutzrechtliche Beurteilung der Fortdauer der Videoüberwachung für erforderlich.

6.14 Bild- und Tonaufnahmen von Versammlungsteilnehmern

In meinem letzten Tätigkeitsbericht (Nr. 5.6.3) hatte ich die Voraussetzungen polizeilicher Bild- und Tonaufnahmen bei Versammlungen dargestellt und berichtet, dass ich die Polizei ausführlich auf diese Rechtslage hingewiesen und um künftige Beachtung gebeten hatte. Zum besseren Verständnis möchte ich nochmals auf die grundlegenden Prinzipien hinweisen:

Die Polizei kann Bild- und Tonaufnahmen zur Strafverfolgung oder zur Gefahrenabwehr anfertigen. Im erstgenannten Fall muss nach der Strafprozessordnung der Anfangsverdacht einer Straftat hinsichtlich der jeweiligen betroffenen Person vorliegen. In letzterem Fall erlaubt §§ 12a, 19a Versammlungsgesetz (VersammlG) die Anfertigung solcher Aufnahmen nur von solchen Versammlungsteilnehmern, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Nicht zulässig ist danach also insbesondere die vorsorgliche Anfertigung von Bildaufnahmen einer Vielzahl von Personen wegen zu erwartender Straftaten oder Gefahrenlagen.

Ich habe gehofft, dass sich die Polizei zukünftig an die gesetzlichen Vorgaben halten werde. Diese Hoffnung wurde aber leider enttäuscht.

Ein Landtagsabgeordneter hat mich über Beschwerden von Bürgern wegen intensiver Videoaufnahmen durch die Polizei anlässlich zweier Versammlungen gegen NPD-Auftritte in München informiert. Diese Information habe ich zum Anlass genommen, eine datenschutzrechtliche Überprüfung der Videografie vorzunehmen.

Bereits bei der Anforderung der Videobänder zur Einsichtnahme bin ich jedoch auf Schwierigkeiten gestoßen. Obwohl die Polizei mir mitgeteilt hatte, die Aufnahmen seien sowohl zur Strafverfolgung als auch zur Gefahrenabwehr angefertigt worden, verweigerte mir die Staatsanwaltschaft die Einsichtnahme in die Videobänder mit der Begründung, diese seien zum Zwecke der Strafverfolgung angefertigt worden. Meine Kontrollkompetenz ruhe daher nach Art. 30 Abs. 4 Satz 1 Bayerisches Datenschutzgesetz (BayDSG) bis zum Abschluss der Strafverfahren. Diese Verweigerung der Unterstützung durch die Staatsanwaltschaft halte ich für rechtswidrig, da die zitierte Rechtsvorschrift meine Kontrolle lediglich bezüglich der Erhebung personenbezogener

Daten durch Strafverfolgungsbehörden bei der Verfolgung von Straftaten beschränkt. Soweit Bildaufnahmen aber - wie hier - ursprünglich nicht zu Zwecken der Strafverfolgung angefertigt wurden, unterliegen sie meiner uneingeschränkten datenschutzrechtlichen Kontrollzuständigkeit. Die Beurteilung der Frage, ob eine repressive oder präventive Datenerhebung vorliegt, und meine Kontrollkompetenz bereits vor Abschluss des strafrechtlichen Ermittlungsverfahrens gegeben ist, ist von mir in eigener Verantwortung zu prüfen.

Ich habe mich deshalb an das Staatsministerium der Justiz gewandt und darum gebeten, die Staatsanwaltschaft zur Erfüllung ihrer gesetzlichen Unterstützungspflicht nach Art. 32 BayDSG anzuhalten. Daraufhin wurden mir schließlich nach Einbeziehung des Innenministeriums die Videobänder ausgehändigt.

Bei meiner anschließenden Prüfung habe ich festgestellt, dass die personenbezogenen Videoaufnahmen bei einer der beiden Versammlungen teilweise, bei der anderen überwiegend unzulässig waren. So wurden bei einer Großdemonstration u.a. einzelne friedliche Versammlungsteilnehmer oder bloße Zuschauer mittels Zoom nahe herangeholt und gefilmt, obwohl weder ein Anfangsverdacht einer Straftat nach § 152 Abs. 2 Strafprozessordnung (StPO) noch Anhaltspunkte dafür vorlagen, dass von ihnen erhebliche Gefahren ausgingen.

Wesentlich schwer wiegender stellte sich jedoch der Eingriff in die unbeeinträchtigte Wahrnehmung des Grundrechts auf Demonstrationsfreiheit bei der zweiten Versammlung dar. Dabei handelte es sich um eine relativ geringe Anzahl von Personen, die aufgelockert zusammenstanden und in ruhiger und absolut friedlicher Weise ihre Meinung z.B. durch Beisichführen einer roten Karte oder durch Diskussionen kundgaben. Die dabei angefertigten Videoaufzeichnungen, auf denen eine Reihe von Versammlungsteilnehmern einzeln, von Nahem und lange andauernd gefilmt wurden, konnten weder auf präventive noch auf repressive Befugnisnormen gestützt werden.

Die Anfertigung von Bild- und Tonaufnahmen zur Gefahrenabwehr ist nur bei einer gesicherten Gefahrenprognose bezüglich der gefilmten Personen zulässig. Die Argumentation der Polizei, man habe befürchtet, dass Personen, die im Vorfeld der Versammlung des Platzes verwiesen worden seien, zurückkehren könnten, greift daher nicht. Die bloße abstrakte Möglichkeit, dass des Platzes verwiesene Personen zurückkehren könnten, reicht für die nach dem Versammlungsgesetz erforderliche Gefahrenprognose bezüglich der von den Videoaufnahmen betroffenen

friedlichen Versammlungsteilnehmern nicht aus. Ggf. hätten im Falle der Rückkehr der von der Verweisung betroffenen Personen diese gefilmt werden dürfen, keinesfalls jedoch die übrigen Versammlungsteilnehmer. Zu keinem Zeitpunkt waren Anhaltspunkte dafür erkennbar, dass gerade von den aufgezeichneten Personen Gefahren ausgehen könnten. Die Situation war aufgrund der geringen Teilnehmerzahl auch überschaubar, die Möglichkeit einer Eskalation war nicht erkennbar.

Die Videoaufzeichnungen können entgegen der Auffassung der Polizei auch nicht auf die repressive Vorschrift des § 100 c Abs. 1 Nr. 1 a StPO gestützt werden, da zum Anordnungszeitpunkt kein Anfangsverdacht einer Straftat vorlag. Die Polizei führte hierzu u.a. aus, man habe die Situation zur Beweissicherung festhalten wollen, um damit das vom Leiter oder Veranstalter der nicht angemeldeten Versammlung begangene Vergehen nach § 26 VersammlG beweissicher verfolgen zu können. Diese Intension rechtfertigt aber die vorgenommene Aufzeichnung nicht. Zur Dokumentation, dass es sich um eine Versammlung handelte, hätte es genügt, für eine begrenzte Zeit Übersichtsaufnahmen des Gesamtgeschehens anzufertigen. Nicht erforderlich war es dafür jedoch, über längere Zeit hinweg einzelne, völlig unauffällige Personen heranzuzoomen und personenbezogen zu filmen.

Angesichts des schwer wiegenden Eingriffs in das Grundrecht der Versammlungsfreiheit und des Rechts auf informationelle Selbstbestimmung habe ich diesen Rechtsverstoß förmlich beanstandet.

Auch in einem weiteren Fall habe ich festgestellt, dass eine polizeiliche Videoaufzeichnung bei einer Versammlung einer Rechtsgrundlage entbehrte. Dabei wurden drei Personen gefilmt, die in satirisch anmutender, bundeswehrähnlicher Kleidung ein Plakat bei sich führten. Auf meine Nachfrage, aus welchem Grund die Videoaufnahmen angefertigt wurden, teilte mir die Polizei zunächst mit, es habe der Verdacht eines Auflagenverstoßes bestanden. Nach Überprüfung des Auflagenbescheids habe ich die Polizei darauf hingewiesen, dass diesem keine Auflage zu entnehmen ist, gegen die die gefilmten Personen verstoßen haben könnten. Daraufhin hat die Polizei die Aufzeichnung damit begründet, es habe aufgrund der Verwendung von Uniformen der Verdacht bestanden, dass der Versammlungsleiter die Versammlung wesentlich anders durchführt, als es in der Anmeldung durch den Veranstalter angegeben war (§ 25 Nr. 1 VersammlG). Im Hinblick darauf, dass in der entsprechenden Anmeldung als Kundgebungsmittel sowohl Satire als auch szenische Darstellungen genannt wurden, habe ich die Polizei darauf hingewiesen, dass

alleine aus dem Umstand, dass drei Personen als zusätzliches Mittel in uniformähnlicher Kleidung erschienen sind, kein Anfangsverdacht für eine Straftat nach § 25 Nr. 1 VersammlG angenommen werden kann. Für eine derartige Annahme müsste die Versammlung oder der Aufzug vielmehr **wesentlich** anders durchgeführt werden, als die Veranstalter bei der Anmeldung angegeben haben. Dies ist jedoch nur dann der Fall, wenn aufgrund der Abweichung eine Lage geschaffen wird, die es nicht mehr ermöglicht, die Veranstaltung hinreichend zu schützen oder wenn die Veranstaltung infolge der abweichenden Durchführung Interessen anderer oder Gemeinschaftsinteressen in unerträglichem Maße beeinträchtigen würde.

Ich habe die Polizei darum gebeten sicherzustellen, dass diese Rechtsauffassung künftig Beachtung findet.

Zusammenfassend habe ich aufgrund meiner Prüfungen den Eindruck gewonnen, dass die Polizei bei Versammlungen auch vorsorglich Videoaufzeichnungen für den Fall anfertigt, dass sich zu einem späteren Zeitpunkt Straftaten ergeben sollten. Einem solchen Vorgehen, das nicht den gesetzlichen Vorgaben entspricht, trete ich jedoch entschieden entgegen. Ich werde daher auch weiterhin durch Kontrollen darauf hinwirken, dass die Polizei die gesetzlichen Voraussetzungen für die Anfertigung von Videoaufnahmen bei Versammlungen beachtet.

6.15 Automatische Gesichtsfeld- und Kennzeichenerkennung

Das Staatsministerium des Innern hatte mich davon in Kenntnis gesetzt, dass die bayerische Polizei Systeme zur automatischen Gesichtsfeld- und Kennzeichenerkennung in Probeversuchen testen wolle. Hierzu wurde ich um Stellungnahme aus datenschutzrechtlicher Sicht gebeten.

Nachdem meine Prüfung keine Bedenken gegen die Gesichtsfelderkennung ergeben hatte, wird sie nunmehr in der polizeilichen Praxis getestet. Dazu wird im Bereich von Grenzkontrollen bei Identitätszweifeln durch Einlesen der Fotos auf dem Ausweis und Ablichtung des Ausweisinhabers überprüft, ob dieser mit der auf dem Ausweis abgebildeten Person identisch ist. Der kontrollierende Beamte erhält als Ergebnis eine computerunterstützte Aussage, mit welcher Wahrscheinlichkeit das Passfoto mit der vorgezeigten Person übereinstimmt und kann dementsprechend über weitere polizeiliche Maßnahmen entscheiden. Es handelt sich damit um eine reine Personenverifikation, bei der das eingelesene Foto nicht mit einer Zentraldatei oder einer sonsti-

gen Datei verglichen wird. Es wird auch weder eine Zentraldatei eingerichtet noch werden die erhobenen Daten über den Abgleichvorgang hinaus gespeichert.

Die automatische Kennzeichenerkennung soll in verschiedenen Bereichen getestet werden. So sollen im Rahmen von Geschwindigkeitsüberwachungen, bei Vorkontrollen zu bestimmten Veranstaltungen, an Grenzübergängen, im Rahmen des Objektschutzes sowie im Rahmen von Fahndungsmaßnahmen die Kennzeichen vorbeifahrender Kraftfahrzeuge eingelesen und automatisch mit dem Fahndungsbestand abgeglichen werden.
Nach Art. 43 Abs. 1 Satz 3 Polizeiaufgabengesetz (PAG) kann die Polizei im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Voraussetzung für einen Abgleich ist demnach, dass die Kraftfahrzeugkennzeichen zunächst zur Erfüllung einer anderen polizeilichen Aufgabe und nicht lediglich zum Zwecke des Abgleichs erlangt worden sind.

Ausgehend davon halte ich aus datenschutzrechtlicher Sicht den geplanten Abgleich im Rahmen der Verkehrsüberwachung für zulässig. Dabei sollen nämlich nicht alle vorbeifahrenden Kraftfahrzeuge mit dem Fahndungsbestand abgeglichen werden, sondern nur diejenigen, die auf Grund einer Geschwindigkeitsüberschreitung ohnehin erfasst werden. Die Kennzeichen dieser Kraftfahrzeuge, die wegen einer Geschwindigkeitsüberschreitung „geblitzt“ werden, sind im Rahmen einer anderweitigen Aufgabenerfüllung der Polizei erlangt und können daher mit dem Fahndungsbestand abgeglichen werden.

Auch soweit die automatische Kennzeichenerkennung an einer Kontrollstelle im Rahmen einer Ringalarmfahndung nach § 111 Strafprozessordnung durchgeführt werden soll, habe ich keine grundsätzlichen Bedenken geäußert. Eine solche Kontrollstelle dient nicht nur der Identitätsfeststellung, sondern auch der Ergreifung des Täters und der Sicherstellung von Beweismitteln und ist daher weiter als Art. 13 PAG. In den Fällen, in denen ein bestimmtes Kraftfahrzeugkennzeichen des flüchtigen Täters bekannt und ausgeschrieben ist, müssen ohnehin alle Kraftfahrzeugkennzeichen zum Zwecke des Abgleichs mit diesem Kennzeichen erhoben werden. Diese im Rahmen der strafverfolgenden Aufgabe der Polizei erhobenen Daten dürfen sodann auch mit dem Fahndungsbestand nach Art. 43 Abs.1 Satz 3 PAG abgeglichen werden. Gleiches gilt für den Fall, dass sich der Straftäter möglicherweise mit einem gestohlenen Kraftfahrzeug auf der Flucht befindet, da dann ebenfalls alle passierenden Kraftfahrzeugkennzeichen erhoben und mit dem gesamten Fahndungsbestand abgeglichen werden. Im Rahmen einer Ringalarmfahndung

hielte ich die automatische Kennzeichenerkennung an Kontrollstellen daher nur dann für unzulässig, wenn feststeht, dass der Straftäter nicht mit einem Kraftfahrzeug auf der Flucht ist. Dann wären die Daten nicht im Rahmen einer anderweitigen Aufgabenerfüllung der Polizei erhoben, sondern ausschließlich zum Zwecke des Abgleichs mit dem Sachfahndungsbestand. Dies wäre nach Art. 43 Abs. 1 Satz 3 PAG aber unzulässig.

Für unzulässig halte ich die Fälle der Kennzeichenerkennung, bei denen die Polizei aus präventivpolizeilichen Gründen die Kennzeichen der passierenden Kraftfahrzeuge gerade zum Zwecke des Abgleichs mit dem Fahndungsbestand erheben will. So wird an zwei Grenzübergängen ab 01.10.2002 eine stationäre Kennzeichenerkennung durchgeführt, bei der jedes vorbeifahrende Kraftfahrzeugkennzeichen erfasst und mit dem Fahndungsbestand abgeglichen wird. Außerdem sollen im Rahmen von Vorkontrollen bei Veranstaltungen für einen bestimmten Zeitraum alle vorbeifahrenden Kraftfahrzeuge abgeglichen werden. Schließlich ist der mobile Einsatz eines Kennzeichenerkennungssystems auch für den Raum bzw. Objektschutz, z. B. vor Wohnblocks von US-Streitkräften, vorgesehen.

Das Innenministerium vertritt hierzu die Auffassung, diese Maßnahmen seien von der Vorschrift des Art. 13 PAG gedeckt, wonach die Polizei die Identität einer Person an den genannten Bereichen feststellen und die Aushändigung eines mitzuführenden Berechtigungsscheins (z. B. Fahrzeugschein) verlangen darf.

Demgegenüber bin ich der Ansicht, dass für diese Fälle derzeit eine gesetzliche Befugnis fehlt. Die mit dem Pilotversuch beabsichtigten Datenerhebungen und Abgleiche haben eine primäre andere Zielrichtung als die vom Innenministerium angeführte Identitätsfeststellung und gegenüber der gesetzlich geregelten Verfahrensweise eine neue Qualität. An Stelle der Durchführung der in Art. 13 PAG vorgesehenen individuellen Personenkontrollen mit evtl. Überprüfung von Berechtigungsscheinen sollen mittels automatisierter Kennzeichenerkennung nur Autokennzeichen erhoben und abgeglichen werden. Darüber hinaus wird durch den automatisierten Kennzeichenabgleich eine lückenlose Überprüfung aller passierenden Kraftfahrzeugekennzeichen ermöglicht, während bei der gesetzlich vorgesehenen Verfahrensweise regelmäßig nur eine stichprobenartige Kontrolle möglich ist.

Hinsichtlich Kontrollmaßnahmen, die auf das Erkennen von Störern abzielen – z.B. die genannten Kontrollmaßnahmen vor speziell gefährdeten Gebäuden oder Einrichtungen durch Abgleich

mit „Gefährderlisten“ -, könnte man als Erhebungs- und Abgleichsbefugnis an Art. 31 i.V.m. Art. 43 PAG denken, wonach zur Gefahrenabwehr Datenerhebungen zulässig sind und diese Daten dann mit anderen Datenbeständen abgeglichen werden können. Art. 31 ist aber derart allgemein gefasst, dass er nach meiner Auffassung eine solche neue und umfassende Datenerhebungsmaßnahme nicht abdecken würde. Auch diese Frage könnte mit der von mir für erforderlich gehaltenen Änderung des PAG geregelt werden.

Ich habe das Innenministerium deshalb auf die Unzulässigkeit der Maßnahme und die Notwendigkeit einer polizeigesetzlichen Regelung hingewiesen. Von einer Beanstandung der bereits praktizierten Kennzeichenerkennung an einer bayerischen Grenze habe ich im Hinblick auf die geringe Eingriffstiefe sowie die befristete Dauer von drei Monaten und ihres Charakters als Pilotversuch abgesehen.

6.16 Präventive Identitätsfeststellung und erkennungsdienstliche Behandlung

Ein Bürger hat sich an mich gewandt, weil er einer polizeilichen Personen- und Fahrzeugkontrolle unterzogen und in diesem Zusammenhang - zum Zwecke der späteren Identifizierbarkeit - mit einer Nummer vor seinem Körper fotografiert worden sei.

Im Rahmen meiner datenschutzrechtlicher Überprüfung hat mir die zuständige Polizeidirektion mitgeteilt, dass es in der Vergangenheit an einer bestimmten Örtlichkeit zu einer größeren Schlägerei zwischen zwei gegnerischen Gruppierungen gekommen sei, bei der einige Personen zum Teil schwer wiegende Verletzungen erlitten hätten. Aufgrund einer Warnung vor Racheakten habe die Polizei intensive Kontrollen durchgeführt. So seien u.a. im Rahmen einer Zufahrtskontrolle im Bereich der besagten Örtlichkeit die Personalien von Personen, die aufgrund der Gesamtumstände möglicherweise als Störer zu dem geplanten Treffen unterwegs gewesen seien, festgestellt und ein Lichtbild angefertigt worden. Die Maßnahmen hätten dazu gedient, die Betroffenen aus der Anonymität herauszureißen und spätere Straftäter nachträglich identifizieren zu können.

Die berichtete Vorgehensweise der Polizei entbehrt einer gesetzlichen Grundlage. Entgegen der Auffassung der Polizeidirektion kann die Anfertigung der Lichtbilder insbesondere nicht auf Art. 32 PAG gestützt werden. Zwar können nach Art. 32 PAG unter bestimmten Voraussetzun-

gen Bildaufnahmen im Zusammenhang mit öffentlichen Veranstaltungen oder an bestimmten Orten angefertigt werden. Die Vorschrift ermächtigt die Polizei aber nur, unter den dort genannten Voraussetzungen **einen Geschehensablauf** auf Video aufzuzeichnen. Die Videoaufzeichnung dient dann z.B. im Fall des Art. 32 Abs. 1 PAG bei evtl. Ausschreitungen als Beweismaterial zur Dokumentation der Situation und ermöglicht der Polizei, anhand der Aufnahmen Störer ausfindig zu machen. Erst danach wird deren Identität ermittelt. Wird jedoch eine Person einzeln - noch dazu unter Vorhaltung einer Nummer - fotografiert und gleichzeitig deren Personalien festgehalten, liegt eine erkennungsdienstliche Maßnahme vor, deren Zulässigkeit sich ausschließlich nach § 81 b StPO und Art. 14 PAG richtet. Sofern die dort genannten Voraussetzungen nicht vorliegen, stellt sich die Maßnahme als unzulässig dar, ein hilfsweiser Rückgriff auf Art. 32 PAG ist ausgeschlossen.

Gegen den Petenten lagen keinerlei Anhaltspunkte hinsichtlich möglicher früherer Straftaten vor. Die Polizei befürchtete lediglich, er könne zu einem späteren Zeitpunkt in Straftaten verwickelt werden. Damit scheidet sowohl § 81 b StPO als auch die ohnehin subsidäre Landesvorschrift des Art. 14 PAG als Rechtsgrundlage für die erkennungsdienstliche Behandlung aus. § 81 b StPO erlaubt die erkennungsdienstliche Behandlung nur bei Beschuldigten, während Art. 14 PAG verlangt, dass der Betroffene verdächtig ist, eine Straftat begangen zu haben.

Ich habe die zuständige Polizeidirektion auf die Rechtslage hingewiesen und darauf aufmerksam gemacht, dass ich eine Beanstandung der Vorgehensweise prüfe. Wegen der grundsätzlichen Bedeutung der Fragestellung hat diese den Vorgang dem Staatsministerium des Innern vorgelegt. Das Innenministerium vertritt die Auffassung, eine Bildaufnahme nach Art. 32 PAG könne gleichzeitig mit einer Identitätsfeststellung nach Art. 13 PAG vorgenommen werden. Der Unterschied zur Anfertigung von Lichtbildern im Rahmen einer erkennungsdienstlichen Maßnahme bestehe darin, dass der Betroffene für diese Maßnahme an- und festgehalten und zur Polizeidienststelle gebracht werden dürfe, dass er an der Durchführung der Maßnahme mitwirken müsse und diese ggf. auch mit Zwangsmitteln durchgesetzt werden könne. Dagegen ermächtige Art. 32 PAG nur zur Anfertigung von Lichtbildern, ohne dass vom Betroffenen eine aktive Mithilfe verlangt werden könne. Als problematisch stelle sich die Vorgehensweise daher nur dann dar, wenn vom Betroffenen verlangt worden sei, sich die Nummer vor den Körper zu halten.

Der Auffassung des Innenministeriums kann ich nicht zustimmen. Die rechtliche Grundlage für die Maßnahme der Polizei kann nicht davon abhängen, ob die Polizei vom Petenten verlangt hat,

sich die Nummer vor den Körper zu halten, ob der Petent dies freiwillig getan hat oder ob die Polizei sie ihm vor den Körper gehalten hat. Zwar ist es zutreffend, dass eine Identitätsfeststellung nach Art. 13 PAG neben oder während einer Bildaufnahme nach Art. 32 PAG durchgeführt werden darf. Wenn die Bildaufnahme und die Identitätsfeststellung aber - wie hier - dergestalt miteinander verknüpft werden, dass sie im Ergebnis einer erkennungsdienstlichen Behandlung gleichkommen, so müssen auch deren besondere gesetzliche Voraussetzungen erfüllt sein.

Unter Darlegung meiner Rechtsauffassung habe ich das Innenministerium erneut um Stellungnahme gebeten.

6.17 Einsatz besonderer Mittel der Datenerhebung

Bei einer Polizeidienststelle habe ich die Vornahme von verdeckten Datenerhebungsmaßnahmen nach Art. 33 Polizeiaufgabengesetz geprüft. Dabei handelt es sich um die längerfristige Observation, den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen sowie zum Abhören oder zur Aufzeichnung des nicht-öffentlich gesprochenen Wortes und den Einsatz von verdeckten Ermittlern.

Diese Maßnahmen sind aufgrund ihres verdeckten Charakters und ihrer Eingriffsintensität in das informationelle Selbstbestimmungsrecht nur unter besonderen gesetzlichen Voraussetzungen zulässig. Bei den von mir geprüften Maßnahmen im Bereich der organisierten Kriminalität lagen diese Voraussetzungen zwar vor, die erforderlichen Anordnungen waren aber nicht in jedem Fall ausreichend präzisiert. So blieb es bei einer Anordnung offen, wer, wie und in welchem Umfang verdeckt videografiert werden sollte. Dies ist aber notwendig, um den konkreten Eingriff in das Recht auf informationelle Selbstbestimmung festzulegen und zu dokumentieren.

Des Weiteren waren die Maßnahmen zwar - wie gesetzlich vorgeschrieben - befristet. Sie waren aber zum Teil für einen sehr langen Zeitraum angeordnet worden. Eine schriftliche Regelung der Befristung des Einsatzes verdeckter Datenerhebungsmaßnahmen ist bei den Polizeidienststellen nicht vorhanden.

Ich bin der Auffassung, dass eine solche Maßnahme grundsätzlich höchstens für die Dauer von drei Monaten angeordnet werden sollte. In begründeten Einzelfällen könnte die Maßnahme nach

erneuter Prüfung und Begründung befristet verlängert werden. Eine solche Befristung der Einzelanordnung auf höchstens drei Monate dient auch der Eigenkontrolle der Polizei. Ich habe deshalb gegenüber der Polizei angeregt, die Anordnungen künftig zu präzisieren, die regelmäßige Höchstdauer einer Anordnung (3 Monate) in einer Dienstanweisung festzulegen und die Überschreitung dieser Höchstdauer in besonderen Einzelfällen schriftlich zu begründen.

Die Polizeidienststelle hat mir ein geändertes Formblatt für die schriftlichen Anordnungen vorgelegt. Dieses enthält datenschutzrechtliche Verbesserungen. Insbesondere die darin vorgesehenen Angaben zu Art, Umfang und Dauer (Befristung) der Maßnahme, aber auch zu deren Anlass und Begründung kommen meiner Forderung nach Präzisierung, Nachvollziehbarkeit und Befristung entgegen. Leider ist die Polizei meiner Forderung nach einer regelmäßigen Anordnungshöchstdauer von drei Monaten nicht gefolgt.

6.18 Entbindung von der Schweigepflicht im Strafverfahren

Bei der Bayerischen Polizei findet seit Jahren das Formblatt „Einwilligung zur Weitergabe personenbezogener Daten“ in einheitlicher Ausgestaltung Anwendung. Durch dessen Unterzeichnung ermächtigen Geschädigte und Zeugen, aber auch Beschuldigte die dort aufgeführten Behörden oder sonstigen Stellen (z. B. Krankenhaus, Arzt, Finanzamt, Geldinstitut), den Ermittlungsbehörden die zur Durchführung des Strafverfahrens erforderlichen Auskünfte über ihre personenbezogenen Daten zu geben sowie die notwendigen Unterlagen zur Verfügung zu stellen. Ausgehend vom bisherigen Inhalt beabsichtigte die Polizei, ein insbesondere vom Layout her verbessertes Formblatt zu erstellen. Diese Gelegenheit habe ich genutzt, meine bereits im Jahre 1996 vorgetragenen, aber damals nicht berücksichtigten Bedenken erneut einzubringen und dadurch auch auf eine inhaltliche Verbesserung in datenschutzrechtlicher Sicht hinzuwirken.

Meine Kritik bezog sich - abgesehen von grundsätzlichen Vorbehalten gegen die Verwendung solcher Formblätter bei Beschuldigten in Strafverfahren - auf die datenschutzrechtlichen Hinweise auf dem Formblatt. Diese heben zwar hervor, dass die Einwilligung freiwillig ist. Nach Art. 15 Abs. 2 BayDSG ist der Betroffene jedoch unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern kann. Die diesbezüglichen Ausführungen in den datenschutzrechtlichen Hinweisen des Formblatts in der derzeitigen Fassung entsprechen diesen Anforderungen nicht, da sie die darzulegenden Rechtsfolgen derart missverständlich darstellen,

dass der Betroffene die Bedeutung und Tragweite seiner Einwilligung sowie die Folgen einer Verweigerung nicht beurteilen kann.

Bei dem gewählten Wortlaut wird für den Betroffenen nicht erkennbar, dass die Polizei in vielen Fällen ohne Zustimmung des Betroffenen keine Möglichkeit hat, die gewünschten Daten zu erhalten. So sind z. B. Geheimnisträger wie Ärzte nach § 203 StGB in der Regel daran gehindert, der Polizei Auskünfte über Patienten zu erteilen. Durch die Formulierung in den datenschutzrechtlichen Hinweisen des Formblatts wird jedoch der Eindruck erweckt, als könne die Polizei die benötigten Informationen von den genannten Stellen auch ohne Zustimmung des Betroffenen mittels richterlichen Anordnungen erhalten, so dass dessen Einwilligung die Einholung von Auskünften lediglich vereinfache und beschleunige.

Ich habe der mit der Erstellung des Formblatts betrauten Stelle daher einen Formulierungsvorschlag für die Fassung der datenschutzrechtlichen Hinweise unterbreitet, durch die derartige Missverständnisse ausgeräumt werden. Indem klar und verständlich darauf hingewiesen wird, dass ohne seine Einwilligung die genannten Behörden und Geheimnisträger nur bei Vorliegen der zum Teil strengen gesetzlichen Voraussetzungen zu Auskünften an die Ermittlungsbehörden berechtigt sind, wird dem Betroffenen seine Wahlmöglichkeit deutlich gemacht. Außerdem wird der Betroffene darauf hingewiesen, dass seine Einwilligung für die Zukunft widerruflich ist.

Die Polizei hatte mir mitgeteilt, das Formblatt sei entsprechend meiner Anregungen geändert worden.

Einige Zeit später hat mich jedoch das Staatsministerium des Innern, das das Formblatt zu genehmigen hatte, darüber informiert, dass es der von der Polizei auf meine Initiative hin vorgeschlagenen Neufassung nicht zugestimmt hat. Daher wurde das bisherige Formblatt inhaltlich vollständig beibehalten und ohne die datenschutzrechtlich notwendigen Änderungen nur vom Layout her verbessert.

Ich halte diese Hinweise für unbedingt erforderlich und werde deshalb eine Beanstandung prüfen.

6.19 Datenübermittlung an die Presse

Auch in diesem Berichtszeitraum habe ich wieder polizeiliche Übermittlungen personenbezogener Daten an die Presse sowohl aufgrund von Zeitungsberichten als auch aufgrund von Bürgereingaben geprüft. In diesem Zusammenhang bin ich erneut an das Innenministerium mit der Frage nach der konkreten Rechtsgrundlage für die allgemeine polizeiliche Pressearbeit herangetreten. Eine spezielle Regelung für diesen wichtigen und besonders sensiblen Bereich existiert nämlich im Polizeiaufgabengesetz nicht, so dass auf eine der allgemeinen Vorschriften zurückgegriffen werden muss. Das Innenministerium vertritt hierzu die Auffassung, es handle sich bei der allgemeinen Pressearbeit um eine polizeiliche Aufgabe, zu deren Erfüllung Art. 41 Abs. 1 Nr. 1 Polizeiaufgabengesetz die Datenübermittlung zulässt. Dem stimme ich zu.

Die allgemeine Öffentlichkeitsarbeit erwächst aus dem im Demokratieprinzip fußenden Prinzip der Transparenz und Publizität des staatlichen Handelns. Wie auch das Innenministerium ausführt, stärkt die allgemeine Pressearbeit das Vertrauen der Gesellschaft in Sicherheitsbehörden und lässt in gewissem Maße eine öffentliche Kontrolle zu. Daneben dient ein Bericht über bestimmte Fälle (z.B. über einen Trickbetrüger und seine Masche) auch zugleich der Warnung und Abschreckung der Öffentlichkeit und damit der Gefahrenabwehr.

Entscheidend für die Rechtsmäßigkeit der Datenübermittlung an die Presse ist aber stets, dass die Persönlichkeitsrechte der Betroffenen ausreichend gewahrt werden. Hierfür bedarf es in jedem Einzelfall einer Abwägung zwischen dem aus Art. 5 Grundgesetz abgeleiteten öffentlichen Informationsinteresse und dem allgemeinen Persönlichkeitsrecht des Betroffenen. Im Rahmen der konkreten Abwägung unter Einbeziehung des hohen Stellenwerts der Pressefreiheit ist daher u.a. zu berücksichtigen, ob eine Information zum Verständnis des Falles unbedingt notwendig ist, ob es sich um eine Information aus der engeren Privatsphäre oder um äußere Umstände handelt und ob die Information einen Täter oder ein Opfer betrifft. Der Betroffene ist dabei grundsätzlich nicht derart konkret oder durch Angaben zu bezeichnen, die einzeln oder in ihrer Gesamtheit zu seiner Identifizierung führen. So kann eine Person auch ohne Angabe des Vor- oder Nachnamens allein durch Angabe des Alters, des Berufs und des Wohnorts für sein soziales Umfeld eindeutig kenntlich gemacht werden. Dies hat die Polizei durch ihre Berichterstattung grundsätzlich zu vermeiden. Besondere Maßgaben gelten für relative oder absolute Personen der Zeitgeschichte.

6.20 Reality-TV

Insbesondere bei privaten Fernsehsendern werden Beiträge über die tägliche Arbeit der Polizei ausgestrahlt. Bei diesen sog. Reality-TV-Sendungen unterrichtet die Polizei, in Einzelfällen auch in Bayern, die Presse vorab über bevorstehende Einsätze und gestattet ihr die Teilnahme daran, sowie die Anfertigung von Bild- und Tonaufzeichnungen. Diese Form der Zusammenarbeit von Polizei und Presse bei der Produktion von Sendungen über polizeiliche Einsätze ist aus datenschutzrechtlicher Sicht problematisch, da die Polizei der Presse personenbezogene Aufnahmen ermöglicht. Solchermaßen aktives und zielgerichtetes Ermöglichen und Fördern von Bild- und Tonaufzeichnungen der Presse durch die Polizei kommt einer polizeilichen Datenübermittlung an Private gleich, die nur unter den jeweiligen gesetzlichen Voraussetzungen (Art. 41 Abs. 1 und Abs. 2 Polizeiaufgabengesetz) zulässig ist.

Bei der Frage, ob die Polizei das Fernsehen überhaupt über bevorstehende Einsätze informieren und daran teilnehmen lassen darf, muss eine Güterabwägung vorgenommen werden. Bei den widerstreitenden Interessen ist auf der einen Seite insbesondere die Art des Einsatzes und die daraus resultierende mögliche Intensität eines Eingriffs in den Persönlichkeitsbereich des Betroffenen zu berücksichtigen (z.B. Begleitung bei normalen Streifengängen oder bei einer Hausdurchsuchung). Auf der anderen Seite steht das legitime Interesse der Öffentlichkeit, das über bloße Neugierde und Sensationslust hinausgehen muss, sowie das Prinzip der Transparenz und Publizität des staatlichen Handelns.

Wenn diese Abwägung ergibt, dass die Beteiligung des Fernsehens grundsätzlich zulässig ist, sollten in jedem Einzelfall folgende Grundsätze beachtet werden:

- Die vom Fernsehen angefertigten Aufnahmen sollten nur eine Übersicht des Vorgangs ermöglichen, ohne den Betroffenen individuell erkennen zu lassen.
- Eine Person darf nur dann erkennbar gefilmt werden, wenn sie zuvor nach hinreichender Aufklärung über den Umfang, die Dauer und den Verwendungszweck der Aufnahmen ihre Einwilligung erklärt hat. Dabei sollte auf die Freiwilligkeit der Aufnahme hingewiesen werden.

- Ist eine Person trotzdem ohne vorherige Einwilligung erkennbar gefilmt worden, so soll derartiges Filmmaterial unverzüglich vernichtet bzw. gelöscht werden, wenn der Betroffene die Einwilligung nachträglich verweigert.
- Auf Grund der besonderen Situation bei der Einwilligung zur Filmaufnahme soll eine zusätzliche schriftliche Einwilligung vor Sendung personenbezogenen Filmmaterials vorgesehen werden.
- Soll das Filmmaterial für einen anderen Beitrag verwendet werden, bedarf es einer erneuten schriftlichen Einwilligung des Betroffenen.
- Die Polizei sollte generell eine Sichtung des fertigen Filmmaterials vornehmen, um bei einer Verletzung von Persönlichkeitsrechten der Betroffenen ggf. einer Veröffentlichung widersprechen zu können.

Um mich über die Handhabung zu informieren hatte ich mich beispielhaft an ein Polizeipräsidium gewandt und mir die dortige Vorgehensweise erläutern lassen. Dabei habe ich festgestellt, dass bei den in diesem Polizeipräsidium mit der Presse geschlossenen Vereinbarungen teilweise Personen erkennbar gefilmt werden konnten, bevor bzw. ohne dass diese in die Aufnahmen eingewilligt haben. Ich habe mich daher unter Darstellung der o.g. Grundsätze an das Innenministerium gewandt und darauf hingewiesen, dass personenbezogene, polizeilich ermöglichte Aufnahmen ohne vorherige Einwilligung des Betroffenen datenschutzrechtlich problematisch sind.

Das Innenministerium hat mir daraufhin mitgeteilt, die Problematik bedürfe einer eingehenden Bewertung unter den Gesichtspunkten der polizeilichen Öffentlichkeitsarbeit und des Datenschutzes. Zusätzlich zu einer eingehenden rechtlichen Prüfung der Erforderlichkeit einer Richtlinie werde sich daher eine Arbeitsgruppe mit der Thematik befassen, um eine einheitliche und praxisgerechte Handhabung bei der bayerischen Polizei zu gewährleisten.

Ich werde die Angelegenheit weiter verfolgen.

6.21 Datenübermittlung an Fahrerlaubnisbehörden

Nach § 2 Abs. 12 Straßenverkehrsgesetz (StVG) hat die Polizei Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaub-

nisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist. Soweit die mitgeteilten Informationen für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind, sind die Unterlagen unverzüglich zu vernichten. Im Berichtszeitraum hat das Innenministerium ein Schreiben mit Vorgaben für den Vollzug dieser Vorschrift an die Regierungen, die Präsidien der Bayerischen Polizei und das Bayerische Landeskriminalamt gerichtet, um die einheitliche Erfüllung der gesetzlichen Informationspflicht sicherzustellen. Darin wird u.a. anhand von Beispielen näher erläutert, wann von einem nicht nur vorübergehenden Mangel hinsichtlich der körperlichen, geistigen oder charakterlichen Eignung oder der mangelnden Befähigung auszugehen ist. Außerdem wird aufgezeigt, wie die Fahrerlaubnisbehörden mit den übermittelten Unterlagen zu verfahren haben.

Ich habe das Innenministerium in zwei Punkten auf datenschutzrechtliche Bedenken aufmerksam gemacht:

So habe ich darauf hingewiesen, dass die Vorgaben insofern irreführend sind, als sie den Schluss nahe legen, dass eine Straftat dann an die Fahrerlaubnisbehörde zu melden sei, wenn sie **entweder** im Zusammenhang mit dem Straßenverkehr **oder** mit der Kraftfahreignung steht. Diesbezüglich habe ich hervorgehoben, dass eine Straftat, die keinen Einfluss auf die Eignung zum Führen von Kraftfahrzeugen hat und daher nicht mit dieser im Zusammenhang steht, nicht übermittelt werden darf, da eine derartige Information für die Fahrerlaubnisbehörde zur Überprüfung der Eignung nicht erforderlich sein kann. Ich habe daher angeregt diese Rechtslage klarzustellen.

Ferner habe ich hinsichtlich des Verfahrens bei der Fahrerlaubnisbehörde in den Fällen, in denen der Betroffene zwar keine Fahrerlaubnis besitzt oder beantragt hat, aber mit einer Antragstellung mit großer Wahrscheinlichkeit zu rechnen ist, auf eine Unstimmigkeit hingewiesen. Während ausdrücklich dargestellt wurde, dass die übermittelte Information nur so lange aufbewahrt werden darf, wie nach den Umständen des Einzelfalls mit **hoher Wahrscheinlichkeit** mit einer Antragstellung **in absehbarer Zeit** zu rechnen ist, wurde gleichzeitig als diesbezügliche Höchstfrist 10 Jahre angegeben. Ich habe hierzu ausgeführt, dass bei einem derart langen Zeitraum nicht mehr von einer hohen Wahrscheinlichkeit mit einer Antragstellung in absehbarer Zeit gesprochen werden kann und habe daher - auch im Hinblick auf die Gefahr einer pauschalen Handhabung - die Streichung der Angabe einer Höchstfrist gefordert.

Das Innenministerium hat die Vorgaben zum Vollzug des § 2 Abs. 12 StVG entsprechend meinen Anregungen abgeändert, so dass diese keinen Bedenken mehr begegnen.

6.22 Übermittlung von Prostituiertendaten an Gesundheitsämter

Vor dem Hintergrund des zum 01.01.2001 in Kraft getretenen Infektionsschutzgesetzes (IfSG) hat das Staatsministerium für Gesundheit, Ernährung und Verbraucherschutz eine Bekanntmachung zum Vollzug des § 19 IfSG und des Polizeiaufgabengesetzes (PAG) herausgegeben, die an die Stelle von Bekanntmachungen zur früheren Rechtslage tritt. Darin werden neben den Aufgaben des Gesundheitsamts bezüglich der durch sexuelle Kontakte übertragbaren Krankheiten auch Vorgaben für die polizeiliche Aufgabenerfüllung in Bezug auf Prostitution allgemein und diesbezügliche Datenübermittlungen an Gesundheitsämter im Besonderen dargestellt.

Der mir zunächst übermittelte Entwurf sah vor, dass die Polizei dem Gesundheitsamt Personen, welche die Prostitution ausüben, meldet, um den Gesundheitsämtern die aufsuchende Beratung oder infektionsschutzrechtliche Anordnungen zu ermöglichen. Als Rechtsgrundlage für diese Datenübermittlung wurde Art. 40 Abs. 3 PAG genannt.

Ich habe das Staatsministerium für Gesundheit, Ernährung und Verbraucherschutz darauf hingewiesen, dass nach In-Kraft-Treten des Infektionsschutzgesetzes eine derart pauschale Übermittlung sämtlicher Personen, die der Prostitution nachgehen, nicht mehr zulässig ist.

Nach Art. 40 Abs. 3 PAG darf die Polizei von sich aus lediglich dann bei ihr vorhandene personenbezogene Daten an andere Behörden oder öffentliche Stellen, die für die Gefahrenabwehr zuständig sind, übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint. Nach der bis zum 31.12.2000 geltenden Rechtslage waren sämtliche Prostituierte aufgrund von § 4 Abs. 1 Geschlechtskrankheitengesetz verpflichtet, dem Gesundheitsamt ein Gesundheitszeugnis vorzulegen. Die daraus resultierende Verpflichtung, sich in regelmäßigen Abständen einer Untersuchung durch das Gesundheitsamt zu unterziehen, konnte von Seiten des Gesundheitsamts mit Zwangsmitteln durchgesetzt werden. Ausgehend hiervon hatte die Polizei die Personalien der Prostituierten nach Art. 40 Abs. 3 PAG dem Gesundheitsamt mitzuteilen.

Mit Einführung des IfSG wurde jedoch der generelle Zwang zu ärztlichen Untersuchungen abgeschafft. Das IfSG setzt vielmehr auf das Angebot freiwilliger Beratung und Untersuchung durch die Behörden des öffentlichen Gesundheitsdienstes. Die Gesundheitsämter können nur noch dann infektionsschutzrechtliche Anordnungen treffen, wenn im Einzelfall Erkenntnisse darüber vorliegen, dass eine Person durch ihr Verhalten Gesundheit und Leben anderer gefährdet. Sie bedürfen daher zur Erfüllung ihrer Aufgaben auch nicht mehr der Übermittlung sämtlicher Personen, die der Prostitution nachgehen. Eine pauschale Datenübermittlung nach Art. 40 Abs. 3 PAG ist damit unzulässig.

Ich habe daher eine Änderung der Bekanntmachung dahingehend gefordert, dass die Polizei die Personalien von Prostituierten nur dann an das Gesundheitsamt übermitteln darf, wenn im Einzelfall aufgrund konkreter Anhaltspunkte der Verdacht besteht, dass die Person andere gesundheitlich gefährdet, so dass das Gesundheitsamt Anordnungen treffen könnte.

Das Staatsministerium für Gesundheit, Ernährung und Verbraucherschutz hat meine Forderung aufgegriffen und die Bekanntmachung entsprechend geändert.

Das Innenministerium hat gegen die Änderung jedoch Bedenken geäußert, da diese zu einem Rückgang der dem Gesundheitsamt zur Verfügung stehenden Datenmenge führe und dadurch eigeninitiativ durch das Gesundheitsamt kein Kontakt mehr zu der möglichen Zielgruppe für das aufsuchende Angebot über Beratung und Untersuchung aufgenommen werden könne. Hierdurch könne das Ziel des Infektionsschutzgesetzes, die Bekämpfung von gefährlichen Krankheiten und somit der Schutz der Bevölkerung vor solchen Erkrankungen, nicht gewährleistet werden. Das Innenministerium hat daher angeregt, von den betroffenen Behörden diesbezügliche Erfahrungswerte einzufordern und ggf. eine Umformulierung der Bekanntmachung in Betracht zu ziehen.

Demgegenüber habe ich auf die Intention des Gesetzgebers bei Erlass des IfSG hingewiesen und eine der gesetzlichen Regelung widersprechende Vollzugsregelung abgelehnt. Der Bundesgesetzgeber war ausweislich der Gesetzbegründung der Auffassung, der Infektionsschutz sei durch Aufklärung und Eigenverantwortung der Prostituierten besser zu erreichen als durch äußeren Zwang. Eine namentliche Erfassung und Zwangsberatung scheidet daher nach der derzeitigen Gesetzeslage aus.

6.23 Auskunft über präventive Speicherungen bei laufenden Ermittlungsverfahren

In meinem letzten Tätigkeitsbericht (Nr. 5.8.4) hatte ich dargestellt, dass die Polizei Bürger mit ihren Auskunftsbegehren über die zu ihrer Person gespeicherten Daten an die zuständige Staatsanwaltschaft verweist, wenn ein Tatvorwurf in einem anhängigen Ermittlungsverfahren im Kriminalaktennachweis gespeichert ist. Das Innenministerium vertritt die Auffassung, Art. 48 Polizeiaufgabengesetz (PAG) umfasse nicht die Daten eines noch anhängigen Strafverfahrens, auch wenn diese Daten in polizeilichen Dateien zu präventiven Zwecken gespeichert würden, da hierfür alleine die Regelungen des Strafverfahrens maßgebend seien.

Ich hatte demgegenüber darauf hingewiesen, dass die Polizei als speichernde Stelle die datenschutzrechtliche Verantwortung trägt und dementsprechend ihrer grundsätzlichen Auskunftsverpflichtung nach Art. 48 PAG nachzukommen hat. Die Entscheidung gegenüber dem Bürger, ob ein gesetzlicher Auskunftsverweigerungsgrund vorliegt ist daher von der Polizei und nicht von der Staatsanwaltschaft zu treffen. Dabei hatte ich gegenüber dem Innenministerium auch ausgeführt, dass durch eine interne Abstimmung zwischen Polizei und Staatsanwaltschaft der Gefahr einer „Aushebelung“ der Entscheidungsbefugnisse der Staatsanwaltschaft über die Auskunftserteilung aus einem laufenden Ermittlungsverfahren entgegengewirkt werden kann. So könne die Polizei die Auskunft nach Art. 48 Abs. 2 PAG grundsätzlich verweigern, wenn die Staatsanwaltschaft ihr Einvernehmen mit einer Auskunftserteilung an den Betroffenen aus Gründen der Gefährdung der Zwecke des Strafverfahrens ablehnt.

Die von mir in dieser Angelegenheit im letzten Tätigkeitsbericht angekündigte Abstimmung des Innenministeriums mit dem Justizministerium hat zu einem Vorschlag des Innenministeriums geführt, den ich ablehne. Danach soll die Polizei die Auskunft stets verweigern, wenn die Staatsanwaltschaft in einem laufenden Ermittlungsverfahren kein Einverständnis zur Auskunftserteilung erklärt hat. Außerdem soll künftig generell bei der Erledigung von Auskunftsersuchen bei der Polizei darauf hingewiesen werden, dass die Auskunft bezüglich laufender Ermittlungsverfahren nur erfolgt, soweit die zuständige Staatsanwaltschaft hierzu ihr Einvernehmen erteilt hat. Dadurch solle der Gefahr einer Ausforschung durch eine Negativauskunft vorgebeugt werden.

Ich habe mich auch gegen einen jeder Auskunftserteilung pauschal anzufügenden Hinweis, wonach die Auskunft im Falle eines laufenden Ermittlungsverfahrens möglicherweise unvollständig

ist, ausgesprochen. Hierdurch bliebe für den Betroffenen stets unklar, ob tatsächlich keine Daten gespeichert sind oder nur eine unvollständige bzw. gar keine Auskunft erteilt wird. Ich habe das Innenministerium darauf hingewiesen, dass dies der gesetzgeberischen Entscheidung in Art. 48 Abs. 1 PAG widerspricht, wonach dem Betroffenen grundsätzlich Auskunft zu erteilen ist, sofern dem nicht im Einzelfall die im Gesetz genannten Gründe entgegenstehen.

Als Reaktion auf meine Ausführungen hat mir das Innenministerium mitgeteilt, dass nunmehr geprüft werde, ob eine Änderung des Art. 48 PAG erforderlich sei.

Derartige Überlegungen entbinden die Polizei jedoch nicht von der Verpflichtung, über die Erteilung von Auskünften bis zum evtl. In-Kraft-Treten einer verfassungskonformen Neureglung nach der derzeitigen Rechtslage zu entscheiden.

6.24 Generelle Auskunftsablehnung bei Betäubungsmittelhandel

In meinem letzten Tätigkeitsbericht (Nr. 5.8.3) hatte ich die Problematik der Auskunftserteilung bei Betäubungsmittelhandel dargestellt. Nach Art. 48 Abs. 2 Nr. 1 Polizeiaufgabengesetz (PAG) wird dem Betroffenen keine Auskunft über die zu seiner Person gespeicherten Daten erteilt, soweit eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei, zu besorgen ist. Ausgehend hiervon sehen die Richtlinien der Polizei vor, dass ohne Einzelfallprüfung in allen Fällen des unbefugten Rauschgifthandels eine Auskunft unterbleibt.

Diese Regelung steht mit der Gesetzeslage nicht in Einklang. Ein entscheidender Bestandteil des Grundrechts auf informationelle Selbstbestimmung ist für den Bürger die Möglichkeit, sich zu informieren, welche öffentliche Stelle was über ihn weiß. Ohne entsprechende Kenntnis hat der Bürger keine Möglichkeit, eventuelle Ansprüche, z.B. auf Berichtigung oder Löschung, durchzusetzen. Eine Verweigerung der Auskunftserteilung kann daher nur in besonderen Ausnahmen in Betracht kommen nach Beurteilung des Einzelfalls und unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes. In den Fällen des unbefugten Rauschgifthandels ist dabei zu beachten, dass es sich um Sachverhalte handelt, die nach Art und Umfang derart verschieden sind, dass bei einer Auskunftserteilung nicht stets von einer Gefährdung der polizeilichen Aufgabenerfüllung ausgegangen werden kann. Im übrigen wird die Durchführung des Strafverfahrens dem Betrof-

fenen in vielen Fällen bereits bekannt sein, so dass eine Geheimhaltung der polizeilichen Speicherung nicht erforderlich ist.

Die in dieser Angelegenheit mit dem Innenministerium geführten Besprechungen und die seinerzeit vom Ministerium und von mir unterbreiteten Vorschläge hatte ich bereits in meinem letzten Tätigkeitsbericht dargestellt. Zuletzt hatte das Innenministerium vorgeschlagen, dass bei leichteren Fällen des unbefugten Rauschgifthandels gemäß § 29 Abs. 1 Nr. 1 Betäubungsmittelgesetz (BtMG) eine Auskunft erteilt werden könne, wenn eine Gefährdung der polizeilichen Aufgabenerfüllung in Folge der Auskunftserteilung nicht zu besorgen sei.

Eine derartige Regelung lehne ich ab, da sie der gesetzlichen Vorgabe des Art. 48 PAG aus mehreren Gründen widerspricht. Zum einen besteht nach Art. 48 PAG eine Auskunftspflicht, so dass die Auskunft in den dort genannten Fällen nicht nur erteilt werden **kann**, sondern zu erteilen **ist**. Zum anderen wird die Möglichkeit zur Auskunftserteilung durch die vom Innenministerium gewählte Formulierung lediglich für Fälle des Grunddelikts des § 29 Abs. 1 Nr. 1 BtMG, nicht jedoch für Fälle des Handels mit sogenannten nicht geringen Mengen (§§ 29 a ff. BtMG), eingeräumt. Eine solche nicht geringe Menge liegt jedoch z. B. bei der weichen Droge Haschisch von durchschnittlicher Qualität bereits bei einer Menge von ca. 100 gr. vor. Eine solche Menge erlaubt für sich gesehen nicht den generellen Schluss, dass bei Auskunftserteilung stets eine Gefährdung der polizeilichen Aufgabenerfüllung zu besorgen sei, so dass eine generelle Auskunftsablehnung nicht in Betracht kommen kann. Schließlich würde durch die vorgeschlagene Formulierung das gesetzliche Verhältnis von Regel und Ausnahme ins Gegenteil verkehrt, da eine Auskunft lediglich dann erteilt werden soll, wenn eine Gefährdung der polizeilichen Aufgabenerfüllung hierdurch nicht zu besorgen ist. Dies bedeutet, dass in Fällen, in denen weder besondere Umstände für noch gegen eine Gefährdung der Aufgabenerfüllung sprechen, eine Auskunft nicht erteilt werden kann, so dass die Auskunft letztlich nur dann erteilt würde, wenn die Prüfung ausnahmsweise positiv ergibt, dass kein Auskunftsverweigerungsgrund vorliegt.

Nachdem ich das Innenministerium auf diese Bedenken hingewiesen hatte, fand erneut ein Gespräch statt, in dessen Folge ich erneut einen Regelungsvorschlag unterbreitete. Da das Betäubungsmittelgesetz den Begriff der leichteren Fälle des Betäubungsmittelhandels nicht kennt und dessen Aufnahme in die Richtlinien daher zu einer erheblichen Unsicherheit bei der Einordnung der jeweiligen Speicherung im Einzelfall führen würde, habe ich mich für eine klare Regelung anhand der verschiedenen gesetzlichen Tatbestände ausgesprochen. Danach soll bei bestimmten,

konkret benannten Tatbeständen, die ich als leichtere Fälle ansehe, Auskunft zu erteilen sein, während die Auskunftserteilung bei den anderen, schweren Fällen grundsätzlich unterbleibt. Ich habe durch meinen Formulierungsvorschlag aber auch hervorgehoben, dass in beiden Fällen die Prüfung des Einzelfalls zu einem anderen Ergebnis führen kann.

Nach einer längeren Prüfung hat mir das Innenministerium nunmehr mitgeteilt, zur Erhaltung des Sicherheitszustands in diesem Deliktsbereich und unter Berücksichtigung datenschutzrechtlicher Erfordernisse sei eine Änderung des Art. 48 PAG in die Wege geleitet worden.

Der Änderungsentwurf bleibt abzuwarten. Das Innenministerium wird dabei aber die Schranken zu beachten haben, die sich aus der Auskunft als wesentlicher Bestandteil der Realisierungsmöglichkeit des Grundrechts auf Datenschutz ergeben.

6.25 Abfragen polizeilicher Informationssysteme

Bereits in meinen beiden letzten Tätigkeitsberichten habe ich mich mit der Problematik von Abfragen polizeilicher Informationssysteme befasst, die das soziale Umfeld des Polizeibediensteten betreffen.

Die von mir vorgeschlagenen Maßnahmen zur Verbesserung des Schutzes gegen Missbrauch, wie z. B. die Einbindung eines Vorgesetzten vor der Datenabfrage, hatte das Staatsministerium des Innern abgelehnt. Ich hatte daraufhin gebeten, diese Maßnahmen wenigstens als Empfehlung an die Polizeidienststellen weiterzugeben. Auch dies hat das Innenministerium u. a. mit der Begründung abgelehnt, dass dadurch bei einzelnen Beamten negative Auswirkungen auf die Motivation zur Durchführung dienstlich veranlasster Maßnahmen und Akzeptanzprobleme hinsichtlich datenschutzrechtlicher Regelungen zu befürchten seien.

Diese Begründung halte ich nicht für akzeptabel. Zwar gehe auch ich davon aus, dass die Polizeibeamten grundsätzlich gesetzes-, richtlinienkonform und sorgsam mit den Daten der Bürger umgehen. Allerdings sind nicht von ungefähr Hinweise von Bürgern bei mir eingegangen, dass Daten, die nur der Polizei zur Verfügung stehen, von unberechtigten Dritten verwendet werden. Freilich war ein Missbrauchsnachweis in diesen Fällen entweder nicht zu führen oder die Ermittlungen versprachen von vorne herein keinen Erfolg.

Dass aber tatsächlich Missbrauch stattfindet, wurde durch eine kürzlich bei mir eingegangene Eingabe deutlich. Während des Wahlkampfes vor den diesjährigen Kommunalwahlen in Bayern hatte ein bislang Unbekannter einen polizeilichen Dateiausdruck mit den längst gelöschten Daten eines Kommunalpolitikers öffentlich ausgehängt. Aufgrund des Sachverhalts lag die Annahme nahe, dass die personenbezogenen Daten des betroffenen Politikers bereits zu einem früheren Zeitpunkt mit dem Ziel, diesen später öffentlich zu diffamieren, in polizeilichen Informationssystemen abgefragt und ausgedruckt wurden. Leider konnte der Täter bislang nicht ermittelt werden.

Angesichts solcher Vorfälle habe ich kein Verständnis, dass sich das Innenministerium weigert, Maßnahmen, die geeignet sind, die Hemmschwelle gegen den Missbrauch zu erhöhen, wenigstens als Empfehlung an die Polizei weiterzugeben.

7 Verfassungsschutz

Beim Landesamt für Verfassungsschutz (LfV) habe ich im Berichtszeitraum wieder Überprüfungen von Datenerhebungen, -speicherungen und -übermittlungen sowie Auskunftserteilungen bzw. -ablehnungen vorgenommen. Die Prüfungen erfolgten in der Regel anlassunabhängig oder aufgrund von Bürgereingaben. Bis auf wenige Einzelfälle waren die Maßnahmen zulässig. Fehler habe ich - wie schon im letzten Berichtszeitraum - z. B. bei der Verlängerung der Speicherungsfrist ohne Vorliegen eines neuen Erkenntnisdatums und bei der Behandlung von Archivakten festgestellt.

Des Weiteren habe ich wieder die Erstellung von Richtlinien und Errichtungsanordnungen überprüft. Das Landesamt für Verfassungsschutz hat mich stets zeitgerecht beteiligt. Meine datenschutzrechtlichen Verbesserungsvorschläge hat es weitgehend berücksichtigt.

Für die nächste Zeit geplante technische Entwicklungen, die Auswirkungen auf den Datenschutz haben, hat mir das Landesamtes für Verfassungsschutz mitgeteilt. So sollen z. B. das für seine

Aufgabenerfüllung maßgeblich Informationssystem IBA umfassend modifiziert, Notebooks eingesetzt und Unterlagen nach und nach durch elektronische Akten ersetzt werden. Diese Entwicklung werde ich kritisch begleiten.

7.1 Maßnahmen des Landesamts für Verfassungsschutz im Zusammenhang mit der Fahndung nach Terroristen nach dem Attentat am 11. September 2001

Als Reaktion auf die Terroranschläge am 11. September 2001 in den USA ergriff auch das Landesamt für Verfassungsschutz Maßnahmen zur Enttarnung möglicher Schläfer in Bayern. Da die Terrorismusaufklärung einen klassischen nachrichtendienstlichen Aufgabenbereich darstellt, ist das Tätigwerden als solches datenschutzrechtlich unproblematisch. Allerdings begegnet die konkret vom Landesamt für Verfassungsschutz durchgeführte Maßnahme datenschutzrechtlichen Bedenken: Das Landesamt für Verfassungsschutz hat von verschiedenen Stellen die Datenbestände aller Personen, die bestimmte Kriterien erfüllen, angefordert und diese sodann mit eigenen Daten zum Teil maschinell abgeglichen.

Nach dem Bayerischen Verfassungsschutzgesetz (BayVSG) haben öffentliche Stellen dem Landesamt für Verfassungsschutz zwar auf dessen Ersuchen die ihnen bei Erfüllung ihrer Aufgaben bekannt gewordenen Informationen zu übermitteln, soweit das zur Erfüllung der Aufgaben des Landesamts für Verfassungsschutz nach dem BayVSG erforderlich ist. Aufgabe des Verfassungsschutzes in diesem Zusammenhang ist es, Bestrebungen im Geltungsbereich des Grundgesetzes, die gegen die Sicherheit des Bundes oder eines Landes gerichtet sind, zu beobachten. Mit der Anforderung von Daten einer Vielzahl von Personen, auf die lediglich bestimmte, im wesentlichen von den bekannten Terroristen übernommene Merkmale zutreffen, werden jedoch nicht Daten über Personen erhoben, die als Angehörige oder Unterstützer einer solchen Bestrebung anzusehen sind. Vielmehr sollte geklärt werden, ob eine solche Bestrebung festzustellen ist. Kennzeichnend hierfür ist, dass Daten von Personen erhoben werden, bei denen nicht bekannt ist, ob sie extremistische Bestrebungen verfolgen oder unterstützen. Bei dem zumindest weit überwiegenden Teil der Betroffenen wird dies voraussichtlich auch nicht der Fall sein.

Auf diese Bedenken habe ich das Landesamt für Verfassungsschutz hingewiesen. Dabei habe ich auch ausgeführt, dass meiner Ansicht nach eine derart weitreichende Datenerhebung durch das Landesamt für Verfassungsschutz nur mit der Schwere der Gefahr unmittelbar nach den An-

schlägen am 11. September 2001 begründet werden kann, die es rechtfertigen kann, an die Konkretheit der Anhaltspunkte für die mögliche Zugehörigkeit zu einer Bestrebung geringere Anforderungen zu stellen. Ich hatte allerdings auch ausdrücklich hervorgehoben, dass dies nur dann gelten könne, wenn kein maschineller Abgleich der Daten erfolgt. Eine solche Datenerhebung mit anschließendem maschinellen Abgleich ist als Rasterfahndung dem Verfassungsschutz mangels ausdrücklicher gesetzlicher Rechtsgrundlage verwehrt.

Im Rahmen einer Prüfung beim Landesamt für Verfassungsschutz habe ich jedoch festgestellt, dass die erhobenen Daten entgegen der ursprünglich geäußerten Absicht des Landesamts für Verfassungsschutz zumindest zum Teil doch maschinell mit eigenen Dateien abgeglichen wurden. Das Landesamt für Verfassungsschutz vertritt hierzu die Auffassung, die Vorgehensweise sei rechtmäßig, da die ursprüngliche Erhebung nicht zum Zweck des maschinellen Abgleichs stattgefunden haben. Vielmehr sei beabsichtigt gewesen, die Daten händisch abzugleichen. Zur rechtlichen Einordnung der Maßnahme und der Beurteilung ihrer Rechtmäßigkeit müsse aber auf den Zweck der Datenerhebung abgestellt werden.

Dieser Auffassung kann ich nicht zustimmen. Würde man allein auf diese subjektiven Absichten abstellen, könnten erhebliche Unsicherheiten entstehen, da in der Regel nicht nachprüfbar sein wird, welche Absicht bei der Erhebung tatsächlich bestand. Wenn, wie im vorliegenden Fall, zwischen der Datenerhebung und dem Datenabgleich ein enger zeitlicher Zusammenhang gegeben ist, besteht darüber hinaus die Gefahr der Umgehung des Fehlens einer erforderlichen speziellen Befugnis. Hier lag zwischen der Erhebung und dem maschinellen Abgleich lediglich eine relativ kurze Zeitspanne von ca. ein bis zwei Monaten, die den Zusammenhang zwischen Datenerhebung und Datenabgleich nicht unterbrechen kann.

Ich habe deshalb diese rechtswidrige Maßnahme förmlich beanstandet und die Löschung der durch die Rasterung erfolgten Speicherungen gefordert, soweit diese nicht zulässigerweise vom LKA übermittelt werden dürften.

7.2 Der Auskunftsanspruch nach dem Bayerischen Verfassungsschutzgesetz

In meinem letzten Tätigkeitsbericht (vgl. Nr. 6.2.6) hatte ich darauf hingewiesen, dass nach Art. 11 Abs. 1 Satz 1 des Bayerischen Verfassungsschutzgesetzes (BayVSG) kein Anspruch auf

Auskunft über die beim Landesamt für Verfassungsschutz (LfV) in Dateien oder Akten gespeicherten Informationen besteht. Hat jedoch eine Person ein besonderes Interesse an einer Auskunft über die zu ihrer Person gespeicherten Daten, so entscheidet das LfV nach pflichtgemäßen Ermessen über das Auskunftsbegehren. Ich hatte auch dargestellt, dass eine geplante Bewerbung für den öffentlichen Dienst ein derartiges besonderes Interesse an einer Auskunft, das über das bei jedem Bürger vorhandene Interesse an den zu seiner Person bestehenden Speicherungen hinausgeht, begründen kann.

Ausgehend von einem konkreten Fall stellte sich die Frage, welche Voraussetzungen erfüllt sein müssen, damit einem Bürger, der sich auf eine geplante Bewerbung im öffentlichen Dienst beruft, Auskunft erteilt wird. Das LfV hatte den Auskunftsantrag aus zwei Gründen abgelehnt: Zum einen müsse auf Grund des Auskunftsantrags nachvollziehbar sein, dass der Antragsteller im Rahmen des Bewerbungsverfahrens mit einer Beteiligung des LfV rechne. Dabei könne aber nicht die - unzutreffende - Vorstellung mancher Bürger zugrundegelegt werden, der Verfassungsschutz werde bei *jeder* Bewerbung für den öffentlichen Dienst beteiligt. Zum anderen könne die bloße Behauptung, der Antragsteller werde sich im öffentlichen Dienst bewerben, nicht ausreichen. Vielmehr müsse die beabsichtigte Bewerbung glaubhaft gemacht werden.

Ich teile die Auffassung des LfV, dass eine beabsichtigte Bewerbung in geeigneter Weise glaubhaft zu machen ist, um nur vorgeschobene Behauptungen zur Erlangung von Auskünften zu verhindern. In Übereinstimmung mit dem LfV gehe ich davon aus, dass dies z.B. durch Mitteilung der beruflichen Qualifikation und des Tätigkeitsbereichs, für den sich der Auskunftsbegehrende bewerben will, erfolgen kann.

Ich habe das LfV jedoch darauf hingewiesen, dass es meiner Ansicht nach nicht darauf ankommen kann, ob im konkreten Einstellungsverfahren eine Regelanfrage beim LfV durchgeführt wird. Auch wenn dies nicht der Fall ist, kann der Betroffene dennoch ein besonderes Interesse hinsichtlich der beim LfV über ihn gespeicherten Informationen haben. Evtl. Speicherungen beim LfV können nämlich auch zu einem späteren Zeitpunkt für das Arbeits/Beamtenverhältnis im öffentlichen Dienst und damit für die Entscheidung, sich zu bewerben bzw. in den öffentlichen Dienst einzutreten, von Bedeutung sein, wenn sie zu diesem Zeitpunkt im Rahmen einer Sicherheitsüberprüfung oder auf Grund anderer Umstände bekannt werden. Dieser Auffassung hat das LfV zugestimmt.

7.3 Einführung eines neuen Registratursystems

In meinem 19. Tätigkeitsbericht (vgl. Nr. 6.2.5) habe ich von der Absicht des Landesamtes für Verfassungsschutz (LfV) berichtet, ein neues Registratursystem einzusetzen. Das neue Verfahren soll neben der Registratur und Verwaltung von Dokumenten die Aufgabe eines funktional darüber hinausgehenden Dokumentenmanagementsystems („elektronische Akte“, „papierarmes Büro“) übernehmen.

Ich habe die Entwicklung dieses Verfahrens sowohl in technisch-organisatorischer als auch in rechtlicher Hinsicht intensiv begleitet. Dabei habe ich insbesondere eine Errichtungsanordnung gefordert, in der die grundlegenden Festlegungen zu Speicherungsinhalt, - umfang und -fristen zu treffen sind. Als problematisch erwies sich vor allem der Schutz der für das LfV zur Aufgabenerfüllung nach dem Bayerischen Verfassungsschutzgesetz irrelevanten personenbezogenen Unterlagen (z. B. Auskunftsersuchen von Bürgern) vor dem Zugriff der Fachabteilungen. Problematisch deswegen, weil die Registrierung der Dokumente zur ablauforganisatorischen Vereinfachung zum Teil von den Sachbearbeitern übernommen werden soll. Dazu ist es notwendig, den Zugriff der Fachabteilungen auf die Registratur- und Verwaltungsdaten (sogenannte META-Daten) zu gestatten. Diese können z. B. im Betrefffeld auch personenbezogene Daten Dritter enthalten.

Um einerseits eine Realisierung des Verfahrens zu ermöglichen, andererseits aber auch den datenschutzrechtlichen Anforderungen Rechnung zu tragen, habe ich eine Reihe technischer und organisatorischer Maßnahmen gefordert:

- keine technische Möglichkeit einer Volltextrecherche
- Zugriff nur auf Dokumente mit einem Aktenzeichen der eigenen Organisationseinheit
- sofortige Löschung negativ beschiedener Erkenntnisanfragen nach Bearbeitung
- Verbot der Recherche mit personenbezogenen Daten und der fachlichen Recherche auch mit nicht personenbezogenen Daten
- zahlenmäßige Begrenzung der anzeigbaren Trefferanzahl bei einer Recherche
- lückenlose Protokollierung der Abrufe mit den von mir geforderten Protokolldaten
- verstärkte Kontrollen des behördlichen Datenschutzbeauftragten des LfV

Damit konnte eine vertretbare Lösung gefunden werden, der auch das LfV zugestimmt hat.

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

In meinem letzten Tätigkeitsbericht (Ziffer 6.2.7) hatte ich ausgeführt, dass das Urteil des Bundesverfassungsgerichts zu den Abhörmaßnahmen des Bundesnachrichtendienstes nicht nur für die Verwendung von Daten, die aus einer Fernmeldeüberwachung gewonnen wurden, von Bedeutung ist. Vielmehr ergeben sich hieraus nach meiner Auffassung auch für die Behandlung personenbezogener Daten, die durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen - insbesondere durch Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel in Wohnungen - Auswirkungen. Die Feststellungen und Forderungen des Bundesverfassungsgerichts, die für den Schutz von Daten gelten, die durch in Art. 10 GG eingreifende Maßnahmen gewonnen wurden, hat der Bundesgesetzgeber im Berichtszeitraum durch eine Novellierung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 GG) berücksichtigt. Im Anschluss daran hat nunmehr auch der Bayerische Gesetzgeber, der zunächst ein entsprechendes Tätigwerden des Bundesgesetzgebers abwarten wollte, eine Gesetzesänderung eingeleitet. Der Gesetzesentwurf greift in einigen Punkten Forderungen des Bundesverfassungsgerichts aus oben genanntem Urteil auf:

- Das Bundesverfassungsgericht hat die Vorschrift des G 10-Gesetzes alte Fassung, wonach die G 10-Kommission des Bundestages über die Zulässigkeit und Notwendigkeit der Beschränkungsmaßnahmen entscheidet, für unvereinbar mit Art. 10 GG erklärt, da sie nicht hinreichend gewährleistete, dass die Kontrolle den gesamten Prozess der Erfassung und Verwertung der Daten umfasst. Ich hatte das Innenministerium darauf hingewiesen, dass diese Ausführungen auch für die inhaltlich gleichlautende bayerische Vorschrift in Art. 2 des Bayerischen Ausführungsgesetzes zum G 10-Gesetz gelten und dieses daher ebenfalls geändert werden müsse. Dieser Forderung wurde nachgekommen. In Anlehnung an die bundesgesetzliche Novellierung enthält nunmehr auch der Bayerische Gesetzesentwurf die gesetzliche Klarstellung, dass sich die Kontrollbefugnis der bayerischen G 10-Kommission

auch auf die Erhebung, Verarbeitung und Nutzung der nach dem G 10-Gesetz erhobenen oder übermittelten personenbezogenen Daten bezieht.

- Auf meine Anregung hin wurde dem Gesetzesentwurf zum Bayerischen Verfassungsschutzgesetz (BayVSG) eine Protokollierungspflicht auch bei der Übermittlung von Daten an öffentliche Stellen hinzugefügt, um eine hinreichende Kontrolle der Übermittlung zu ermöglichen.

- Bei Daten, die durch den Einsatz besonderer technischer Mittel zur Informationsgewinnung im Schutzbereich der Unverletzlichkeit der Wohnung erlangt werden, ist auf meine Anregung eine ausdrückliche Zweckbindungsregelung im Hinblick auf die Verwendung der Daten in das BayVSG aufgenommen worden.

Leider hat es das Innenministerium abgelehnt, eine Kennzeichnungspflicht für Daten, die durch Abhörmaßnahmen aus Wohnungen gewonnen wurden, einzuführen. Diese Überwachungsmaßnahmen seien in ihrer Intensität verdachtsabhängigen, nicht aber verdachtsunabhängigen strategischen Fernmeldekontrollen gleichwertig. Ich halte diese Argumentation nicht für schlüssig. Das Bundesverfassungsgericht hat zur Begründung der Kennzeichnungspflicht nicht auf die Verdachtslosigkeit der Maßnahme abgestellt, sondern auf die nur dadurch gewährleistete Zweckbindung der gewonnenen besonders sensiblen Daten. Ich halte meine Kritik deshalb aufrecht, vgl. im einzelnen Nr. 1.3.

Der Gesetzesentwurf wurde zwischenzeitlich vom Ministerrat beschlossen und wird im Landtag beraten.

8 Justiz

8.1 Gerichtlicher Bereich

8.1.1 Insolvenzordnung und Bekanntmachungsverordnung

Nach der Insolvenzordnung sind Entscheidungen mit weitreichender Wirkung, wie etwa die Eröffnung des Insolvenzverfahrens, die Anordnung von Verfügungsbeschränkungen oder die Bestellung eines vorläufigen Insolvenzverwalters öffentlich bekannt zu machen, um dem Geschäftsverkehr die Möglichkeit zu geben, sich auf die jeweiligen rechtlichen Folgen einzustellen. Diese öffentliche Bekanntmachung erfolgte bisher durch die Veröffentlichung in einem hierfür bestimmten Blatt, etwa einer Tageszeitung. Um die daraus entstehenden Kosten zu reduzieren, aber auch um die Kenntnisnahme durch interessierte Kreise zu erleichtern, legte die Bundesregierung im Januar 2001 einen Gesetzentwurf vor, der zum Zweck hatte, durch eine Änderung des § 9 Insolvenzordnung eine Veröffentlichung dieser Daten auch über das Internet zu ermöglichen. Eine solche Veröffentlichung im Internet bietet neben den genannten Chancen aber auch erhebliche Risiken, da die verwendeten Daten, einmal publiziert, in ihrer räumlichen und zeitlichen Verbreitung und Auswertung kaum mehr kontrolliert werden können. So stehen auch Daten einer Einzelperson, die einem Verbraucherinsolvenzverfahren unterworfen ist, für jedermann zur freien Verfügung.

Gemeinsam haben wir, die Datenschutzbeauftragten des Bundes und der Länder, die besondere Interessenlage bei der Veröffentlichung von Daten eines Insolvenzverfahrens im Internet im Rahmen einer Entschließung (Entschließung vom 24.04.2001 – Anlage 8) hervorgehoben und besondere Vorkehrungen gegen einen Missbrauch dieser Daten gefordert. Gleichzeitig haben wir gefordert, auch bei der Nutzung des Internet im Bereich der Registergerichte oder bei Zwangsvollstreckungsverfahren auf die besondere Gefährdungssituation für das Recht des jeweils Betroffenen auf informationelle Selbstbestimmung durch technische und organisatorische Maßnahmen Rücksicht zu nehmen. Nicht zuletzt in Reaktion auf diese Entschließung hat der Bundestag der Neuregelung in § 9 Insolvenzordnung eine Verordnungsermächtigung hinzugefügt. Im Rahmen dieser Rechtsverordnung soll das Bundesministerium der Justiz die Einzelheiten der Veröffentlichung in einem elektronischen Informations- und Kommunikationssystem regeln.

Dabei sind insbesondere Löschungsfristen vorzusehen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen unversehrt, vollständig und aktuell bleiben, jederzeit ihrem Ursprung nach zugeordnet werden können und nach dem Stand der Technik durch Dritte nicht kopiert werden können. Gleichzeitig hatte der Bundestag die Bundesregierung gebeten, zu prüfen, wie verhindert werden kann, dass amtlich bekannt gemachte Daten nach Ablauf der Löschungsfrist über das Internet veröffentlicht werden. Im Februar 2002 trat die Verordnung des Bundesministeriums der Justiz zu öffentlichen Bekanntmachungen im Insolvenzverfahren im Internet in Kraft. Hierin ist, neben Löschungsfristen für die zur Veröffentlichung im Internet vorgehaltenen Daten insbesondere bestimmt, dass die Daten bei der Übermittlung an die für die Veröffentlichung zuständige Stelle elektronisch signiert werden müssen, Vorkehrungen für die Unversehrtheit, Vollständigkeit und Aktualität der Daten während der Veröffentlichung getroffen werden müssen und spätestens zwei Wochen nach dem ersten Tag der Veröffentlichung die Daten nur noch auf konkrete Abfrage herausgegeben werden dürfen.

8.1.2 Anordnung über Mitteilungen in Zivilsachen (MiZi)

Die Anordnung über Mitteilungen in Zivilsachen, die detaillierte Regelungen über von Amts wegen veranlasste Übermittlungen personenbezogener Daten an öffentliche Stellen nach dem Justizmitteilungsgesetz enthält (siehe 19. Tätigkeitsbericht Nr. 7.3.1), wurde auch in diesem Berichtszeitraum geändert. Erfreulicherweise wurde bereits in dem Änderungsvorschlag der Landesjustizverwaltungen vom Januar 2001 eine Vielzahl der von mir und den anderen Datenschutzbeauftragten des Bundes und der Länder aufgestellter Forderungen berücksichtigt. Hierzu zählen die regelmäßige Beschränkung von Mitteilungen auf den Entscheidungstenor sowie die Verpflichtung, die Mitteilung in den betreffenden Akten mit Inhalt, Art und Weise der Übermittlung sowie Empfänger zu dokumentieren. Auch wurde durch erläuternde Formulierungen hervorgehoben, dass überschießende Daten des Betroffenen oder Dritter in den Mitteilungen auf das unvermeidbare Maß zu beschränken sind und dass die Mitteilung grundsätzlich nur zu dem Zweck verwendet werden darf, zu dessen Erfüllung sie übermittelt wurde. Diese datenschutzrechtlichen Verbesserungen sind nach Abstimmung der Justizverwaltungen auch umgesetzt worden. Leider fand meine zusätzliche Anregung, im Rahmen der Dokumentation der Mitteilungen auch jeweils diejenigen Tatsachen festzuhalten, die das besondere öffentliche Interesse an einer Mitteilung begründen, keine Berücksichtigung, ebenso wenig mein Vorschlag, für überschießende Daten Dritter ein Verwendungsverbot auf Seiten der empfangenden Stelle festzuschreiben.

Ich habe diese Forderungen daher anlässlich erneuter Änderungsvorschläge durch die Landesjustizverwaltungen im Januar 2002 wieder aufgegriffen. Leider ist eine Übernahme meiner Vorschläge auch in den am 01.10.2002 in Kraft getretenen Änderungen der Mitteilungen in Zivilsachen nicht erfolgt.

8.1.3 Aufbewahrungsbestimmungen

8.1.3.1 Aktenaufbewahrungsgesetz

In meinem 19. Tätigkeitsbericht (Nr. 7.2.1) hatte ich über die bereits seit langem andauernden Bemühungen um eine gesetzliche Regelung für die Aufbewahrung von gerichtlichen Akten der Zivil- und Strafjustiz berichtet. Im Mai 2000 wurde durch die 71. Justizministerkonferenz eine länderoffene Arbeitsgruppe eingesetzt, die bis zur Frühjahrskonferenz 2001 geeignete Vorschläge zur Notwendigkeit einer gesetzlichen Regelung für die Aufbewahrungsbestimmungen im Justizbereich erarbeiten sollte. Diese Arbeitsgruppe stellte zunächst fest, dass eine gesetzliche Regelung nach ihrer mehrheitlichen Auffassung entbehrlich sei. Im Hinblick auf den Erforderlichkeitsgrundsatz sollten aber die Fristen der bundeseinheitlichen Aufbewahrungsbestimmungen überprüft werden. Die Prüfung wurde, nach Sachgebieten aufgeteilt, einzelnen Justizverwaltungen zugewiesen. Eine Zusammenstellung der so erarbeiteten Änderungswünsche durch das federführende Justizministerium Nordrhein-Westfalen liegt bisher noch nicht vor.

Im Juni 2001 beschloss die 72. Justizministerkonferenz eine länderoffene Arbeitsgruppe einzusetzen, die einen Entwurf für ein Aufbewahrungsgesetz erarbeiten soll, in dem die grundsätzlichen Voraussetzungen für die Aufbewahrung von Schriftgut in der Justiz geregelt sind und das die Länder ermächtigt, die Einzelheiten, das heißt die konkreten Fristen in (bundeseinheitlich) abgestimmten Rechtsverordnungen oder Verwaltungsvorschriften zu regeln. Allerdings wurde bisher keine Einigung über die Federführung für dieses neu zu schaffende Aktenaufbewahrungsgesetz erzielt, so dass bisher keine weiteren Vorbereitungen zur Schaffung dieses Gesetzes unternommen wurden.

8.1.3.2 Finanzgerichtsbarkeit

Eine gesetzliche Regelung findet sich allerdings auch für die übrige Fachgerichtsbarkeit bisher nicht. Für den Bereich der Finanzgerichtsbarkeit in Bayern wurde durch das Finanzgericht Nürnberg gemeinsam mit der Generaldirektion der Staatlichen Archive Bayerns der Entwurf einer Aussonderungsbekanntmachung Finanzgerichtsbarkeit erarbeitet, der im Juni 2001 durch das Staatsministerium der Finanzen an die Finanzgerichte München und Nürnberg zur Stellungnahme übersandt wurde. Eine Zusendung dieses Entwurfes an mich erfolgte erst im Juli 2001 auf meine Nachfrage hin. Zu diesem Entwurf habe ich gegenüber dem Staatsministerium der Finanzen auf das grundsätzliche Erfordernis einer gesetzlichen Regelung hingewiesen, wenngleich es zu begrüßen ist, dass die Aufbewahrung und Vernichtung bzw. Löschung von Unterlagen nunmehr zumindest in einer Bekanntmachung geregelt werden soll. Zu dem Entwurf selbst habe ich betont, dass die Aufbewahrung von Verfahrensakten sowie spezifischer Karteien in jedem Fall nur zulässig ist, so lange sie für die Aufgabenerfüllung des Gerichts erforderlich ist. Im Rahmen meines Schriftwechsels mit dem Staatsministerium der Finanzen habe ich dann auch festgestellt, dass für die Speicherung so genannter Stammdateien, die die wesentlichen Verfahrensdaten enthalten, in dem Bekanntmachungsentwurf keine Regelungen vorgesehen sind. Ich habe daher eine entsprechende Änderung der Bekanntmachung gefordert. Eine Rückantwort des Staatsministeriums der Finanzen steht hierzu noch aus.

Weiterhin habe ich gefordert, eine jährliche Überprüfung und Aussonderung der Unterlagen vorzusehen. Der Entwurf der Bekanntmachung hatte diese spätestens alle fünf Jahre vorgesehen, so dass unter Umständen Unterlagen, für die eine Aufbewahrungsfrist von fünf Jahren festgelegt wurde, erst nach bis zu zehn Jahren ausgesondert würden. Das Staatsministerium der Finanzen hat mir hierzu mitgeteilt, dass die für die Aussonderung vorgesehenen Akten von den Finanzgerichten inzwischen jährlich bearbeitet werden.

8.1.3.3 Verwaltungsgerichtsbarkeit

Für die Verwaltungsgerichtsbarkeit wurde im Juli 2000 eine Vereinbarung zwischen dem bayerischen Verwaltungsgerichtshof und der Generaldirektion der Staatlichen Archive Bayerns über Aufbewahrung, Aussonderung, Anbietung, Übernahme und Vernichtung der Unterlagen beim

Bayerischen Verwaltungsgerichtshof und bei den Verwaltungsgerichten des Freistaates Bayern abgeschlossen. Von dieser Vereinbarung habe ich erst auf eigene Nachfrage im Juli 2001 erfahren. Bei ihrer Erarbeitung war ich nicht beteiligt worden. Dementsprechend habe ich mich erst im August 2001 in einem Schreiben an den Präsidenten des Bayerischen Verwaltungsgerichtshofes hierzu äußern können. Auch in diesem Schreiben habe ich auf das grundsätzliche Erfordernis einer gesetzlichen Regelung hingewiesen, wenngleich auch hier zu begrüßen war, dass inzwischen zumindest eine Verwaltungsvereinbarung über die Aufbewahrung und Vernichtung bzw. Löschung der Unterlagen getroffen wurde. Darüber hinaus habe ich darauf hingewiesen, dass die Erforderlichkeit einer Datenspeicherung keine unterschiedliche Beurteilung allein aufgrund des Speichermediums finden kann, so dass die Aufbewahrungsfristen, sofern sie den selben Sachverhalt betreffen, für Papierakten wie für elektronisch gespeicherte Daten gleich sein müssen. Zudem habe ich auch bemerkt, dass die dortige Regelung, dass die Aussonderung und Anbietung von Unterlagen, deren Aufbewahrungsfrist abgelaufen ist, spätestens alle zehn Jahre stattfinden soll, das Risiko birgt, dass Unterlagen, die nur zehn Jahre aufzubewahren sind, tatsächlich 20 Jahre lang bei dem Gericht vorgehalten werden.

Im Rahmen mehrerer Besprechungen mit dem Bayerischen Verwaltungsgerichtshof konnte eine Einigung erzielt werden, dass auch die ausgedruckten Daten des elektronischen Eingangsregisters mit Ablauf der Aufbewahrungsfristen für die zugehörigen Verfahrensakten gelöscht werden sollen. Eine Einigung bezüglich der elektronisch gespeicherten Daten steht noch aus. Im Hinblick auf die Umsetzung der Aufbewahrungsfristen hat der Bayerische Verwaltungsgerichtshof erklärt, dass die Aussonderung zeitnah nach Ablauf der jeweiligen Fristen erfolgen soll.

8.2 Strafverfolgung

8.2.1 Auskunft/Akteneinsicht

Das Recht des Einzelnen auf informationelle Selbstbestimmung schließt sein Recht ein, zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß (BVerfGE 65, 1 ff, 43). Dementsprechend bedeutet Datenschutz auch, dem Betroffenen grundsätzlich Auskunft aus oder Einsicht in diejenigen Akten öffentlicher Stellen zu gewähren, in denen seine personenbezogenen Daten gespeichert sind. Bereits in meinem 18. Tätigkeitsbericht (Nr. 7.3.4) hatte ich über die Auskunft aus staatsanwaltschaftlichen Akten berichtet. Aus einer Vielzahl von Anfragen an mich

ist aber deutlich geworden, dass bei dieser Frage immer noch wesentliche Unsicherheiten bei der Anwendung des Rechts bestehen.

8.2.1.1 Auskunft/Akteneinsicht ohne Verteidiger

Ein Betroffener hatte sich an mich gewandt, da er wünschte, in einem gegen ihn geführten Ermittlungsverfahren, das zwischenzeitlich durch rechtskräftigen Strafbefehl abgeschlossen war, Einsicht in den Verfahrensakt zu nehmen. Sein Begehren begründete er gegenüber der aktenführenden Staatsanwaltschaft mit dem Wunsch, den Vorgang zu überprüfen. Die Staatsanwaltschaft lehnte diesen Antrag ab, da nicht durch einen Verteidiger vertretenen Personen grundsätzlich keine Einsicht in Strafverfahrensakten gewährt werde und der Betroffene darüber hinaus kein besonderes Interesse an der Einsichtnahme dargelegt habe. Diese Auffassung, die sich auf das Fehlen einer ausdrücklichen Regelung zum Recht des nicht von einem Verteidiger vertretenen Betroffenen eines Ermittlungsverfahrens auf Auskunft und Akteneinsicht bis zum Inkrafttreten des Strafverfahrensänderungsgesetzes 1999 bezog verkannte, dass bereits das vom Bundesverfassungsgericht definierte Recht auf informationelle Selbstbestimmung Betroffenen grundsätzlich das Recht gewährt, zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß. Dieses Interesse, zu wissen, welche Daten über einen gespeichert sind, kann der Verfolgung rechtlicher Interessen, wie etwa dem Betreiben eines Wiederaufnahmeverfahrens oder auch nur der eigenen Information über den Erkenntnisstand der Behörde dienen. Darüber hinaus kann durch die Verweigerung einer Akteneinsicht für einen nicht durch einen Verteidiger vertretenen Betroffenen, wie vom Europäischen Gerichtshof für Menschenrechte ausgeführt (EGMR, NStZ 1998, Seite 429 f), dessen Recht auf ein faires Verfahren nach Art. 6 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten sowie sein Recht auf rechtliches Gehör nach Art. 103 Abs. 1 Grundgesetz verletzt werden. Dies habe ich sowohl der betroffenen Staatsanwaltschaft als auch dem Staatsministerium der Justiz mitgeteilt.

Durch die Einfügung eines Abs. 7 in § 147 der Strafprozessordnung mit dem Strafverfahrensänderungsgesetz 1999 wurde zwischenzeitlich zwar festgestellt, dass ein Betroffener Auskünfte aus Strafverfahrensakten zu seiner Person auch ohne anwaltlichen Beistand erhalten kann. Der Betroffene hat allerdings nach dem Gesetzeswortlaut lediglich ein Recht auf ermessensfehlerfreie Entscheidung. Ich habe daher, gerade vor dem Hintergrund, dass nicht nur in diesem Fall die beteiligten Stellen Umfang und Folgen des Rechts auf informationelle Selbstbestimmung ver-

kannt hatten, gegenüber dem Staatsministerium der Justiz gefordert, bei der Neufassung der bundesweit einheitlichen Richtlinien für Straf- und Bußgeldverfahren (RiStBV) ausdrücklich darauf hinzuweisen, dass dieses Recht auf ermessensfehlerfreie Entscheidung sich nach rechtskräftigem Abschluss des Verfahrens regelmäßig zu einem Recht auf Erteilung von Auskunft oder Abschriften verdichten wird, ohne dass es einer weiteren Begründung bedarf. Diese Forderung fand jedoch im Rahmen der Beratungen des RiStBV-Ausschusses keine Mehrheit.

8.2.1.2 Auskunft über Datenübermittlungen im Rahmen der Dienstaufsicht

Ein Betroffener hatte bei der gegen ihn ermittelnden Staatsanwaltschaft angefragt, ob dem zuständigen Generalstaatsanwalt über dieses Ermittlungsverfahren im Rahmen der Dienstaufsicht berichtet und damit Daten über seine Person übermittelt worden seien. Die angeschriebene Staatsanwaltschaft wie auch der betroffene Generalstaatsanwalt teilten ihm daraufhin mit, dass ihm über derartige „interne“ Vorgänge, auch sofern sie seine Person betreffen, keine Auskunft gegeben werde. Dies ergebe sich bereits aus der Bezeichnung „intern“.

Von dem Betroffenen angeschrieben habe ich mich an die Staatsanwaltschaft gewandt und dieser dargelegt, dass eine Auskunft über die Übermittlung personenbezogener Daten an den Generalstaatsanwalt dem Betroffenen gegenüber bei Maßnahmen im Rahmen der Strafprozessordnung gemäß § 147 StPO und bei sonstigen Datenübermittlungen gemäß Art. 10 Bayerisches Datenschutzgesetz erteilt werden muss. Gerade im Hinblick auf die nicht in der Strafprozessordnung geregelten Informationen des Generalstaatsanwaltes etwa im Rahmen der allgemeinen Berichterstattung zur Unterstützung der Dienstaufsicht gemäß § 147 Gerichtsverfassungsgesetz habe ich deutlich gemacht, dass der Generalstaatsanwalt hierbei Dritter im Sinne von Art. 4 Abs. 10 Satz 1 Bayerisches Datenschutzgesetz ist und somit eine Datenübermittlung vorliegt, über die, mangels anderweitiger Regelung, gemäß Art. 10 Bayerisches Datenschutzgesetz, unter Berücksichtigung der Einschränkungen in dessen Absätzen 5 und 6 Auskunft zu erteilen ist. Das zwischenzeitlich eingeschaltete Staatsministerium der Justiz hat meine Auffassung bestätigt.

8.2.1.3 Auskunft aus staatsanwaltschaftlichen Dateien

Mit dem Strafverfahrenänderungsgesetz 1999 (siehe 19. Tätigkeitsbericht Nr. 7.1.5) wurden Regelungen für staatsanwaltschaftliche Dateien in die Strafprozessordnung eingeführt und dem

Betroffenen in den §§ 491, 495 Strafprozessordnung ein Auskunftsrecht entsprechend § 19 des Bundesdatenschutzgesetzes gegeben. Zur Unterstützung einer einheitlichen Handhabung bei der Auskunftserteilung bayerischer Staatsanwaltschaften aus der Verfahrensdatei der Behörde sowie aus der landesweiten Datei STARIS hatte das Staatsministerium der Justiz erwogen, Auskünfte nur zu erteilen, wenn sie sich auf abgeschlossene oder den Betroffenen bereits bekannt gegebene Ermittlungsverfahren beziehen. Dazu sollten sämtliche Anfragen durch die Registerbehörde folgende Erklärung enthalten:

> „Aus Gründen der ordnungsgemäßen Aufgabenerfüllung der Staatsanwaltschaften können Auskünfte aus dem [...] staatsanwaltschaftlichen Verfahrensregister nur erteilt werden, wenn sie sich auf abgeschlossene oder dem Betroffenen bereits bekannt gegebene Ermittlungsverfahren beziehen. Insoweit enthält das [...] staatsanwaltschaftliche Verfahrensregister über sie keine bzw. folgende Eintragungen: ...“

Ich habe mich gegen eine derartige generelle Vorgehensweise gewandt. Eine solche, nicht am Einzelfall orientierte Entscheidung würde dem Gesetz nicht entsprechen, das den Betroffenen grundsätzlich einen Anspruch auf Auskunft einräumt, sofern dem nicht im Einzelfall die im Gesetz genannten Gründe entgegenstehen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Das Vorliegen dieser Voraussetzungen ist in jedem Einzelfall vor einer Auskunftsablehnung zu prüfen und zu entscheiden. Eine generelle Auskunftsverweigerung in den oben genannten Fällen würde auch der besonderen Bedeutung des Auskunftsrechts für die individuelle Entfaltung des Einzelnen (siehe BVerfGE 65, 1 ff, 42 f) nicht gerecht. Die Auskunftserteilung ist Voraussetzung für eventuelle Berichtigungs-, Löschungs- und Schadensersatzansprüche, die ohne Kenntnis der Speicherung nicht wahrgenommen werden können. Eine generelle Auskunftsverweigerung ist auch nicht deswegen gerechtfertigt, weil in allen zur Auskunftsverweigerung vorgesehenen Fällen vom Vorliegen von Ablehnungsgründen auszugehen ist. Dies gilt vor allem nicht in den Fällen, in denen gar keine Speicherungen vorhanden sind. Aber auch in den Fällen, in denen noch nicht abgeschlossene bzw. den Betroffenen noch nicht bekannt gegebene Ermittlungsverfahren gespeichert sind, sind Sachverhalte denkbar, in denen eine Auskunftsverweigerung nicht gerechtfertigt ist. So z. B. wenn der Betroffene in einem Ermittlungsverfahren aufgrund offenkundig nicht gegebener Tatbestandsmäßigkeit nicht als Beschuldigter vernommen wurde, das Verfahren aber noch nicht eingestellt ist. Im übrigen in Fällen, in denen keine Anhaltspunkte dafür vorliegen, dass eine Mitteilung des Verfahrens nachteilige Auswirkungen haben könnte.

Das Staatsministerium der Justiz hat gegenüber meiner Kritik darauf hingewiesen, dass gerade auch die Mitteilung, dass keine Speicherungen vorhanden sind, Ermittlungen gefährden könnte. Dies ergebe sich daraus, dass ein derartiges Auskunftsverhalten die Möglichkeit für Rückschlüsse eröffne, wenn in anderen Fällen von der Registerbehörde unter Hinweis auf ermittlungstaktische Erwägungen die Auskunft verweigert wird. Anlässlich der Prüfung einer Staatsanwaltschaft wurde mir mitgeteilt, dass dort mit Ausnahme gesperrter Verfahren eine vollständige Auskunft über die Eintragungen in Verfahrensregister gegeben werde. Eine pauschale Auskunftsverweigerung bezüglich noch nicht abgeschlossener und dem Betroffenen noch nicht bekannt gegebener Verfahren erfolgte dort nicht, weil die Gefahr einer Ausforschung nicht gesehen würde.

Ich habe dem Staatsministerium der Justiz dies mitgeteilt und überdies auf die Rechtsprechung des Bundesverfassungsgerichtes hingewiesen (Beschluss vom 10.10.2000, DVBl 2001, 275 ff., 277), in der das Gericht es als unzulässig ansieht, dass zur Vermeidung einer Ausforschung die Auskunft schematisch, auch bei Fehlen jeglicher Daten, verweigert wird, um so Rückschlüsse auf die Datenspeicherung durch die Differenzierung zwischen Negativauskunft und Auskunftsverweigerung zu vereiteln. Die Auskunft dürfe nur aufgrund konkreter Einzelfallentscheidungen verweigert werden. Die Verweigerung müsse grundsätzlich auch begründet werden. Eine bloße Wiederholung des Gesetzestextes oder der pauschale Verweis auf eine Gefährdung des Zwecks des Auskunftsverweigerungsrechtes wäre hierbei nicht ausreichend. Dennoch hat auch die von mir geprüfte Staatsanwaltschaft ihr bisheriges Auskunftsverhalten dahingehend geändert, dass Auskünfte aus den staatsanwaltschaftlichen Verfahrensregistern nur noch erteilt werden, wenn sie sich auf abgeschlossene oder dem Betroffenen bereits bekannt gegebene Ermittlungsverfahren beziehen. In einem gemeinsam mit dem Freistaat Thüringen im November 2001 in den Bundesrat eingebrachten Gesetzesantrag forderte die Staatsregierung zudem eine Änderung der gesetzlichen Regelung in § 491 Abs. 2 Strafprozessordnung dergestalt, dass eine Auskunft generell nicht erteilt wird, sofern sie sich auf bei der Staatsanwaltschaft noch nicht erledigte Verfahren bezieht. Die Regelung sollte somit über das bisher Geforderte hinausgehen und dem Betroffenen eine Dateiauskunft selbst dann verwehren, wenn ihm das Verfahren bereits bekannt gegeben wurde. Der Bundesrat hat jedoch im März 2002 beschlossen, diesen Gesetzentwurf nicht beim Bundestag einzubringen. Vor diesem Hintergrund habe ich mich erneut an das Staatsministerium der Justiz gewandt und eine Anpassung der Praxis der Auskunftserteilung an die geltende Rechtslage gefordert. In seiner Antwort hat das Staatsministerium der Justiz darauf verwiesen, dass § 491 Abs. 2 StPO bereits in der bestehenden Fassung keine Einzelfallprüfung erfordere.

Diese Auffassung lehne ich ab, da sie der zitierten Rechtsprechung des Bundesverfassungsgerichtes widerspricht.

Zur Klärung der Frage, ob durch Anfragen beim bundesweiten Zentralen Staatsanwaltschaftlichen Verfahrensregister die Gefahr einer Ausforschung gegeben ist, hat die Bundesregierung das Bundeszentralregister beauftragt, eine Statistik über die Auskunftsersuchen Betroffener zu führen. Aufgrund der so gewonnenen Erkenntnisse soll nach Ablauf von zwei Jahren geprüft werden, ob sich die dortige Praxis der vollständigen Auskunftserteilung bewährt hat oder ob eine Gesetzesnovellierung erforderlich ist.

8.2.2 Telekommunikationsüberwachung

8.2.2.1 §§ 100 g, 100 h StPO

Bereits die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in einer Entschließung vom 22./23.10.1996 gefordert, herkömmliche Eingriffsbefugnisse in das Fernmeldegeheimnis nicht ungeprüft unter wesentlich veränderten Bedingungen auf die neuen Formen der Individual- und Massenkommunikation zu übertragen. Vor allem § 12 des damaligen Fernmeldeanlagengesetzes (FAG) sollte durch eine normenklare gesetzliche Regelung in der Strafprozessordnung ersetzt werden, die dem Verhältnismäßigkeitsgrundsatz auch unter den neuen Bedingungen, insbesondere der zunehmenden Bedeutung von Verbindungs- und Bestandsdaten für das Persönlichkeitsrecht des Betroffenen Rechnung trägt (siehe 17. Tätigkeitsbericht Nr. 7.4.1). Diese Forderung nach einer ausdrücklichen gesetzgeberischen Entscheidung über die Herausgabe von Verbindungsdaten, in der auch die veränderten technischen und sozialen Gegebenheiten der Telekommunikation berücksichtigt werden, haben die Datenschutzbeauftragten des Bundes und der Länder anlässlich der 58. Datenschutzkonferenz (Entschließung vom 07./08.10.1999, 19. Tätigkeitsbericht Anlage 8) und der 59. Datenschutzkonferenz (Entschließung vom 14./15.03.2000, 19. Tätigkeitsbericht Anlage 18) wiederholt. Eine Entscheidung über die Neuregelung war auch deswegen angezeigt, weil die nur noch befristete Gültigkeitsdauer des § 12 FAG zuletzt am 31.12.2001 ablaufen sollte. Im August 2001 legte die Bundesregierung den Entwurf einer Nachfolgeregelung zu § 12 Fernmeldeanlagengesetz in Form der §§ 100 g , 100 h Strafprozessordnung vor.

In meiner Stellungnahme gegenüber dem Staatsministerium der Justiz habe ich den Entwurf grundsätzlich begrüßt, da er die Auskunft über Verbindungsdaten der Telekommunikation endlich in den Gesamtzusammenhang der Strafprozessordnung einordnet. Erfreulich war auch, dass durch eine Anlehnung an die Systematik der Telekommunikationsüberwachung in den §§ 100 a, 100 b Strafprozessordnung wesentliche Schutzmechanismen wie die Bindung an einen beschränkten Straftatenkatalog, die grundsätzliche Anordnung durch einen Richter und Unterrichtungs- und Vernichtungspflichten gewährleistet wurden. Dennoch habe ich das Staatsministerium der Justiz auch auf bestehenden Verbesserungsbedarf hingewiesen. Insbesondere fehlen Regelungen über eine Dokumentation aller Fälle der Weitergabe oder zweckändernden Nutzung so erlangter Daten, wie sie durch das Bundesverfassungsgericht in seinem Urteil zur Fernmeldeüberwachung durch den Bundesnachrichtendienst verlangt wurden (siehe 19. Tätigkeitsbericht Nr. 7.2.4.2).

Die Staatsregierung hat meine Anregungen im Rahmen des Gesetzgebungsverfahrens nicht aufgegriffen. Vielmehr wurde in den Beratungen des Bundesrates eine Vielzahl von Änderungen beantragt, die im Vergleich zu dem vorgelegten Gesetzentwurf wesentliche datenschutzrechtliche Verschlechterungen beinhaltete. So wurde grundsätzlich für eine Beibehaltung der bestehenden Regelung in § 12 Fernmeldeanlagengesetz plädiert und ein Wegfall der Beschränkung auf Straftaten von erheblicher Bedeutung bzw. den Straftatenkatalog des § 100 a Strafprozessordnung gefordert. Auch sollte die Überwachung des Standortes eines Mobiltelefons ohne bestehende Verbindung mit einem anderen Teilnehmer gestattet werden. Letztlich konnten diese Forderungen des Bundesrates aber nicht durchgesetzt werden. Zum 01. Januar 2002 trat die neue Regelung der §§ 100 g, 100 h Strafprozessordnung in Kraft.

8.2.2.2 Dokumentation von Telekommunikationsüberwachungsmaßnahmen

In meinem 19. Tätigkeitsbericht (Nr. 7.2.4.2 und Nr. 7.2.4.3) habe ich darauf hingewiesen, dass Eingriffe in das Fernemeldegeheimnis durch Telekommunikationsüberwachungsmaßnahmen der Strafverfolgungsbehörden einer besonderen Dokumentation bedürfen, um eine zureichende Kontrolle der Speicherung, Zweckänderung und Übermittlung zu gewährleisten sowie um sicherzustellen, dass gesetzlich vorgeschriebene Unterrichtungspflichten erfüllt werden. Im Sinne einer gleichmäßigen und grundrechtsfreundlichen Vorgehensweise habe ich gegenüber dem Staatsministerium der Justiz auf die Schaffung eines bayernweit einheitlichen Vordruckes für die

Dokumentation von Telekommunikationsüberwachungsmaßnahmen im Rahmen der Strafverfolgung gedrungen. Nach einer Erhebung der bisher in einzelnen Staatsanwaltschaften verwendeten Formblätter hat das Staatsministerium der Justiz einen eigenen Vorschlag eines Dokumentationsbogens erstellt, bei dessen Entwurf ich beteiligt wurde. Darin sollen die einzelnen Unterlagen, die Weitergabe von Abschriften, die Benachrichtigung Beteiligter sowie die vorschriftsmäßige Vernichtung der Unterlagen nachgewiesen werden. Dabei werden auch Maßnahmen nach § 100 g Strafprozessordnung berücksichtigt. Dieses Formblatt sollte nach meiner Auffassung bei sämtlichen Staatsanwaltschaften in Bayern verwendet werden. Zumindest sollten davon abweichende Vordrucke um die im Vergleich zu dem Entwurf des Staatsministeriums der Justiz fehlenden Felder ergänzt werden. Auch das Staatsministerium der Justiz hat dies in einem Schreiben an die Generalstaatsanwälte bei dem Bayerischen Obersten Landgericht und bei den Oberlandesgerichten München, Nürnberg und Bamberg zum Ausdruck gebracht.

8.2.3 Aufbewahrung besonders sensibler Daten

Anlässlich einer Änderung der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) im Juli 2000 wurde in dessen Nr. 220 formuliert, dass zu Beweiszwecken gefertigte Lichtbilder von Verletzten einer Straftat, die diese ganz oder teilweise unbekleidet zeigen, gesondert in den Akten aufzubewahren sind, um sie bei der Gewährung von Akteneinsicht an Dritte ggf. vorübergehend entfernen zu können. Ich habe gegenüber dem Staatsministerium der Justiz darauf hingewiesen, dass ein entsprechender Schutz für solche Lichtbilder auch gelten muss, wenn diese, etwa durch den Täter selbst, nicht zu Beweiszwecken gefertigt wurden. Dementsprechend habe ich eine Erweiterung der RiStBV gefordert.

Dieser besondere Schutz vor einem unbefugten Zugriff insbesondere im Rahmen der Akteneinsicht durch Dritte muss jedoch auch für andere personenbezogene Daten von vergleichbarer Sensibilität gelten. In Folge dessen habe ich in meiner Stellungnahme zur Änderung der RiStBV eine gesonderte Heftung auch für Sozialdaten und Erkenntnisse aus einer Überwachung der Telekommunikation gemäß §§ 100 g, 100 h Strafprozessordnung (vormals § 12 FAG), die ebenfalls einer besonderen Zweckbindung unterliegen, gefordert. Gleiches habe ich für Erkenntnisse aus präventiven Speicherungen der Polizei angeregt, in denen Tatvorwürfe aufgenommen werden, die zwar nicht zu einer strafrechtlichen Ahndung geführt haben, bei denen aber ein Tatverdacht verblieben ist. Da auch Dritte bei einer Einsicht in den Strafverfahrensakt in derartigen Speiche-

rungen, für die nur ein Verdacht erforderlich ist und bei denen das zugrundeliegende Verfahren sogar durch Freispruch abgeschlossen sein kann, erlangen könnten, habe ich eine gesonderte Aufbewahrung und ggf. Herausnahme bei der Akteneinsicht Dritter verlangt.

Während die gesonderte Aufbewahrung sämtlicher Lichtbilder ganz oder teilweise unbekleideter Verletzter übernommen wurde, hat der RiStBV-Ausschuss die getrennte Abheftung für die anderen von mir genannten Daten nicht übernommen. Neu aufgenommen wurde dagegen, dass

- medizinische und psychologische Gutachten mit Ausnahme solcher von Behörden oder Gerichtsärzten
- Berichte der Gerichts- und Bewährungshilfe sowie anderer sozialer Dienste und
- Niederschriften über die in § 477 Abs. 2 Satz 2 Strafprozessordnung genannten Ermittlungsmaßnahmen

gesondert zu heften und hinsichtlich der Einsichtsgewährung einer besonderen Prüfung zu unterziehen sind. Ich halte dies für eine wesentliche datenschutzrechtliche Verbesserung.

8.2.4 Anordnung über Mitteilung in Strafsachen (MiStra)

Zur Umsetzung des zweiten Abschnittes des Einführungsgesetzes zum Gerichtsverfassungsgesetz regelt eine bundesweit einheitliche Anordnung über Mitteilungen in Strafsachen (MiStra) die Mitteilung personenbezogener Daten von Amts wegen durch Staatsanwaltschaft oder Gericht an öffentliche Stellen für andere Zwecke als die des Strafverfahrens, für die sie erhoben wurden. Diese Anordnung wird regelmäßig durch einen Ausschuss der Justizverwaltungen auf Änderungsbedarf hin überprüft.

In Reaktion auf die Regelung des § 477 Abs. 2 Satz 2 Strafprozessordnung, dass Erkenntnisse aus besonders eingriffsintensiven Maßnahmen einer besonderen Zweckbindung unterliegen, habe ich gegenüber dem Staatsministerium der Justiz gefordert, in der MiStra vorzuschreiben, dass derartige Erkenntnisse, auch soweit sie in den Entscheidungsgründen enthalten sind, nur unter den engen Voraussetzungen des § 477 Abs. 2 Satz 2 Strafprozessordnung übermittelt werden dürfen. Liegen diese Voraussetzungen nicht vor, so sollen keine Entscheidungsgründe mitgeteilt werden. Der MiStra-Ausschuss ist dieser Forderung nicht gefolgt, obwohl die Staatsanwalt-

schaften in Hamburg und dem Saarland bereits nach dieser Maßgabe verfahren. Ich habe dementsprechend darum gebeten, diese Vorgehensweise zumindest im Rahmen einer internen Anweisung für Bayern vorzusehen. Das Staatsministerium der Justiz hat diesbezüglich jedoch einen Regelungsbedarf verneint.

Da mehrere Forderungen der Datenschutzbeauftragten des Bundes und der Länder bereits wiederholt bei Änderungen der MiStra nicht berücksichtigt wurden, hat sich der derzeitige Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem gemeinsam abgestimmten Schreiben an den Vorsitzenden der Justizministerkonferenz gewandt und auf nach unserer Auffassung besonders wichtige Punkte hingewiesen:

- Sofern eine Mitteilung über ein Strafverfahren nach der gesetzlichen Vorgabe erst nach einer individuellen Bewertung bspw. über das Vorliegen eines öffentlichen Interesses erfolgt, soll der Betroffene über diese Übermittlung der Daten informiert werden.
- Die Entscheidung über eine Mitteilung aus dem Strafverfahren soll, sofern sie aufgrund einer individuellen Bewertung erfolgt, besonders qualifizierten Amtsträgern vorbehalten werden.
- Die Mitteilungen sollen nur stattfinden, sofern hierfür auf Seiten des Empfängers ein konkreter und ausreichender Bedarf besteht und nur in dem Umfang, der für die Aufgabenerfüllung des Empfängers erforderlich ist.
- Mitteilungen über die Einstellung eines Verfahrens gemäß § 170 Abs. 2 Strafprozessordnung wegen Schuldunfähigkeit des Betroffenen sollen, wenn diese nur vorübergehender Natur war, das zugrundeliegende Gutachten älter als fünf Jahre ist oder weitere Ermittlungen nicht zur Erhebung der öffentlichen Klage führen würden, unterbleiben. Die Betroffenen sollen über derartige Mitteilungen unterrichtet werden.

Ich habe das Staatsministerium der Justiz über dieses Schreiben unterrichtet und um Unterstützung der darin genannten Anliegen gebeten.

8.2.5 Geschäftsstellenautomation bei den Staatsanwaltschaften

Die Geschäftsstellenautomation bei den Staatsanwaltschaften ist bereits seit längerem Gegenstand intensiver Korrespondenz zwischen mir und der Justizverwaltung (siehe 18. Tätigkeitsbe-

richt Nr. 7.2). Bereits im Jahre 1997 hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder von ihrem Arbeitskreis Justiz vorgeschlagene datenschutzrechtliche Forderungen zum Einsatz von automatisierten staatsanwaltschaftlichen Informationssystemen zur Kenntnis genommen (18. Tätigkeitsbericht Nr. 7.2.1.2). Die Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz hat daraufhin eine Arbeitsgruppe mit der Erörterung dieser Forderungen beauftragt. Die Arbeitsgruppe erstattete im Mai 2000 ihren Bericht, der den Landesjustizverwaltungen und dem Bundesministerium der Justiz durch die Bund-Länder-Kommission als Grundlage bei der Weiter- und Neuentwicklung von Vorgangsverwaltungs- und -bearbeitungssystemen für Staatsanwaltschaften und deren Kommunikation mit den zentralen Registern empfohlen wurde. Der Bericht stimmt in vielen Punkten den von uns aufgestellten Forderungen zu. In manchen Punkten vertritt er jedoch eine abweichende Auffassung. Im Hinblick auf die unterschiedlichen Bewertungen in einzelnen Punkten habe ich mich in einem mit den anderen Datenschutzbeauftragten des Bundes und der Länder abgestimmten Schreiben an den Vorsitzenden der Justizministerkonferenz gewandt und darin unsere Anliegen insbesondere zu eigenständigen Löschungsfristen für die Daten Geschädigter, die Beschränkung des Datenumfanges bei einem Zugriff externer Stellen, Zugriffsbeschränkungen auf Daten Strafunmündiger und der Opfer von Sexualdelikten sowie die Protokollierung sämtlicher auch nur lesender Zugriffe verdeutlicht. Die Arbeitsgruppe der Bund-Länder-Kommission hat sich auch mit diesem Schreiben auseinandergesetzt. Hierbei konnte in einigen Punkten eine Klarstellung und Annäherung der Standpunkte erreicht werden. Dennoch habe ich mich in einzelnen Punkten zu einer Stellungnahme gegenüber dem Staatsministerium der Justiz veranlasst gesehen. Dies gilt insbesondere für die fortdauernde Weigerung der Arbeitsgruppe, die Daten Strafunmündiger, der Opfer von Sexualdelikten oder auch von Mitbeschuldigten, deren Unschuld ausdrücklich festgestellt wurde, generell zu sperren. Auch habe ich erneut auf die Notwendigkeit einer Protokollierung auch lesender Zugriffe zum Zwecke der Prävention und zur Nachvollziehbarkeit im Falle unberechtigter Zugriffe hingewiesen. Das Justizministerium hat ausgeführt, dass die von der Arbeitsgruppe verweigerte Datensperre bei einem Vorgang gegen Strafunmündige und bei festgestellter Unschuld in Bayern als „freiwillige datenschutzfreundliche Regelung“ bereits umgesetzt ist und dass die Protokollierung lesender Zugriffe in der Strafprozessordnung nicht vorgeschrieben sei.

Die Anforderungen an die Geschäftsstellenautomation der Staatsanwaltschaften habe ich dem Staatsministerium der Justiz auch bei dessen Abfassung einer Mustererrichtungsanordnung für das in Bayern verwendete System SIJUS-STRAF-StA dargelegt. Gemäß § 490 Satz 1 Strafprozessordnung war den Staatsanwaltschaften bis zum 01.11.2001 die Schaffung einer Errichtungs-

anordnung für automatisierte Dateien aufgegeben. Das Staatsministerium der Justiz hat den Staatsanwaltschaften für SIJUS-STRAF-StA ein Muster formuliert und zur Übernahme zur Verfügung gestellt. Im Rahmen der Schaffung dieser Mustererrichtungsanordnung, bei der ich vom Justizministerium beteiligt wurde, musste ich bedauerlicherweise feststellen, dass das System SIJUS-STRAF-StA zwischenzeitlich gravierende Veränderungen erfahren hatte, ohne dass ich hiervon informiert worden war. Ich habe demzufolge darum gebeten, mich im Hinblick auf den datenschutzrechtlichen Bezug dieses Verfahrens bei Abänderungen in Zukunft frühzeitig zu beteiligen und mich über die aktuelle Version auf dem Laufenden zu halten. Weiterhin habe ich die Ausweitung der Speicherungsfristen für die Daten von Nebenbeteiligten wie Zeugen, Anzeigenerstatter und Geschädigte von zunächst einem Monat seit Weglegung der Akten auf nunmehr ein bzw. fünf Jahre kritisiert. Diese Verlängerung, die mit Bedürfnissen beim Auffinden der Akten begründet wurde, ist um so schwerwiegender, als nicht einmal eine Reduzierung der gespeicherten Daten auf das für die Aktensuche unbedingt Erforderliche vorgesehen ist. Auch für die Daten von Betroffenen und Beschuldigten findet eine derartige Teillöschung nicht statt. Das Staatsministerium der Justiz hat mir hierzu mitgeteilt, dass meine Forderungen im Rahmen der Fortentwicklung von SIJUS-STRAF-StA geprüft werden. Auch soll auf meine Anregung hin überprüft werden, ob die Daten einzelner Mitbeschuldigter, die bereits in einem frühen Verfahrensstadium als Täter ausgeschieden sind und gegen die das Verfahren wegen Unschuld eingestellt wurde, nicht bereits zu einem früheren Zeitpunkt gelöscht werden könnten als die Daten der anderen Beschuldigten, gegen die ggf. ein noch lange andauerndes Verfahren fortgeführt wird. Ein Ergebnis dieser Prüfung wurde mir bisher noch nicht mitgeteilt.

8.2.6 Viertes Bundeszentralregisteränderungsgesetz

Eine Änderung des Bundeszentralregistergesetzes war bereits seit längerem Gegenstand von Überlegungen (siehe 18. Tätigkeitsbericht Nr. 7.1.6) ohne bisher realisiert worden zu sein. Im März 2000 legte das Bundesministerium der Justiz erneut einen Referentenentwurf eines Vierten Gesetzes zur Änderung des Bundeszentralregistergesetzes vor. Das Staatsministerium der Justiz hat mich hieran erfreulicherweise bereits in diesem frühen Stadium des Gesetzgebungsverfahrens beteiligt. Der Gesetzentwurf beinhaltete im Wesentlichen eine Neuregelung für die Behandlung von Entscheidungen über die Einstellung eines Verfahrens wegen erwiesener oder vermuteter Schuldunfähigkeit. Dahingehende Eintragungen im Bundeszentralregister wurden bisher praktisch lebenslang vermerkt. Nach der Neuregelung sollen sie nach Ablauf bestimmter

Fristen aus dem Register entfernt werden, was ich begrüße. Weiterhin soll sie Änderungen wie die Festschreibung von Berichtigungs- und Nachberichtspflichten bei festgestellter Unrichtigkeit der mitgeteilten Daten bewirken und eine Rechtsgrundlage für die Einführung eines automatisierten Mitteilungs- und Auskunftsverfahrens schaffen.

In meiner Stellungnahme gegenüber dem Staatsministerium der Justiz habe ich darauf hingewiesen, dass der Gesetzentwurf in vielen Punkten meinen bereits in vorangegangenen Gesetzgebungsverfahren dargelegten Forderungen entspricht. So das Erfordernis, dass Eintragungen einer auf Schuldunfähigkeit des Betroffenen basierenden Entscheidung nur stattfinden sollen, wenn die Feststellungen über die Schuldunfähigkeit auf einem aktuellen Sachverständigengutachten beruhen und die Ermittlungen im Übrigen genügenden Anlass zur Erhebung der öffentlichen Klage geboten hätten, da für derart gravierende Eintragungen mindestens der gleiche Sorgfaltsmaßstab zu gelten hat, wie für andere Eintragungen. Darüber hinaus habe ich auf weitere änderungsbedürftige Punkte hingewiesen, insbesondere die Notwendigkeit, die Bedingungen des automatisierten Abrufverfahrens, eine enge Beschränkung des Teilnehmerkreises daran und die Pflicht, sämtliche Abrufe zu protokollieren, klarzustellen, sowie darauf, dass abweichende Personendaten, wie frühere Namen im Falle einer Adoption oder einer Geschlechtsumwandlung nur in ein Führungszeugnis aufgenommen werden sollen, sofern dabei ein Bezug zu den sonstigen Eintragungen des Führungszeugnisses besteht. In Reaktion auf den endgültigen Gesetzentwurf der Bundesregierung sowie Empfehlungen des Unterausschusses Recht des Bundesrates habe ich in einer ergänzenden Stellungnahme gegenüber dem Staatsministerium der Justiz zusätzlich deutlich gemacht, dass eine längerfristige Eintragung von Entscheidungen, die auf der Schuldunfähigkeit des Betroffenen basieren, nur dann akzeptiert werden kann, wenn die Schuldunfähigkeit nicht, wie etwa bei einer Vollrauschtat, nur vorübergehender Natur war. In dem auf Empfehlung des Vermittlungsausschusses beschlossenen Gesetz wurden die von mir hervorgehobenen Forderungen nur teilweise aufgegriffen. So führten meine Anregungen für das automatisierte Abrufverfahren sowie mein Hinweis auf eine Differenzierung zwischen dauernder und nur vorübergehender Schuldunfähigkeit bei Eintragungen im Bundeszentralregister zu keiner Änderung. Dafür wurde in Bezug auf die Mitteilung abweichender Personaldaten festgelegt, dass derartige Mitteilungen in Führungszeugnissen für Private keinen Eingang finden sollen und in Führungszeugnissen für Behörden nur, wenn sie für dort angegebene Eintragungen von Bedeutung sind. Im Hinblick auf die oben dargestellten Verbesserungen gerade bei der Eintragung von Entscheidungen, die von der Schuldunfähigkeit des Betroffenen ausgehen, halte ich das Gesetz für eine erfreuliche Verbesserung im Sinne des Datenschutzes.

8.2.7 EUROJUST

Im Oktober 1999 hat der Europäische Rat in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 01. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden zur Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen erheben, verarbeiten und nutzen soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. Im Hinblick darauf sind umfassende Datenschutzvorschriften erforderlich. Die Konferenz der Datenschutzbeauftragten des Bunds und der Länder hat demgemäß im Oktober 2001in einer Entschließung hierauf hingewiesen und Regelungen sowohl zur Verarbeitung, Speicherung, Nutzung, Berichtigung und Löschung personenbezogener Daten als auch zum Auskunftsanspruch der Betroffenen sowie zu einer Kontrollinstanz für EUROJUST gefordert (Entschließung der 62. DSK vom 24. bis 26.10.2001 – Anlage 18). Hierbei wurden besondere Voraussetzungen für eine Weitergabe von Daten an Dritte und detaillierte Regelungen über Umfang und Dauer insbesondere automatisierter Speicherungen gefordert. Im Interesse des einzelnen Betroffenen soll diesem ein eigener Auskunftsanspruch gegenüber EUROJUST und angemessener Rechtsschutz gewährt und darüber hinaus durch eine gemeinsame unabhängige Kontrollinstanz die Einhaltung des Datenschutz garantiert werden.

Anlässlich einer Sitzung des Arbeitskreises Justiz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im November 2001 in München konnten unsere Anregungen auch gegenüber dem deutschen Delegationsleiter in der Ratsarbeitsgruppe EUROJUST dargelegt werden, der dem Arbeitskreis über den Stand der Arbeiten berichtete. Nachdem in den Beratungen innerhalb der Europäischen Union unsere Anliegen zumindest teilweise berücksichtigt worden

waren, hat der Rat der Justiz- und Innenminister den Beschluss über die Errichtung von EUROJUST im Dezember 2001 gebilligt.

8.3 Justizvollzug

8.3.1 Briefkontrolle

Wie bereits in meinem 19. Tätigkeitsbericht (Nr. 7.4.1, Ziffer 2) geschildert, hatte ich in einer Justizvollzugsanstalt festgestellt, dass die Staatsanwaltschaft, in deren Zuständigkeitsbereich die Justizvollzugsanstalt liegt, Schreiben an dort Inhaftierte in einem Sammelumschlag ohne weitere Sicherung der einzelnen Schriftstücke verschickt und in Folge dessen die Justizvollzugsanstalt bei deren Aushändigung zwangsläufig von dem Inhalt jedes einzelnen Schreibens Kenntnis nehmen kann. Ich hatte mich deswegen sowohl an die Justizvollzugsanstalt als auch an die Staatsanwaltschaft gewandt und darauf hingewiesen, dass nach den gesetzlichen Bestimmungen eine Überwachung des Briefwechsels nur für den Einzelfall aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erfolgen darf und deshalb jedes Schreiben einzeln verschlossen werden müsse. In ihrer Antwort an mich hat die Staatsanwaltschaft die fehlende Sicherung mit der generellen Überprüfung eingehender Post in der betreffenden Justizvollzugsanstalt gerechtfertigt, weshalb die Anstalt ohnehin von jedem eingehenden Schreiben unabhängig von der Art des Transportes Kenntnis erlange.

Aufgrund der grundlegenden Bedeutung der Frage einer generellen Überwachung des Briefverkehrs habe ich mich an das Staatsministerium der Justiz gewandt und darauf hingewiesen, dass bereits das Bundesverfassungsgericht deutlich gemacht hat, dass § 29 Abs. 3 Strafvollzugsgesetz, der die Überwachung des Schriftwechsels gestattet, im Lichte der besonderen Bedeutung des Brief- und Postgeheimnisses, am Einzelfall orientiert und unter strenger Berücksichtigung des Verhältnismäßigkeitsgrundsatzes auszulegen ist. Da jedoch in mehreren obergerichtlichen Urteilen eine generelle Überwachung des Schriftwechsels in einzelnen Anstalten aufgrund der dortigen Verhältnisse für zulässig erachtet wurde, habe ich um Mitteilung derjenigen Kriterien gebeten, nach denen eine Entscheidung über die vollständige Überwachung ein- und ausgehenden Schriftverkehrs in den Justizvollzugsanstalten in Bayern erfolgt. Das Staatsministerium der Justiz hat mir hierzu mitgeteilt, dass die Überwachung des Briefverkehrs mit Privatpersonen bei sämtlichen Gefangenen einer Anstalt damit begründet wird, dass einzelne Gefangene, bei denen eine Gefährdung von Sicherheit oder Ordnung der Anstalt zu besorgen ist, ihre individuelle

Kontrolle ansonsten durch die Einschaltung anderer Gefangener umgehen könnten. Gleiches gelte für Untersuchungsgefangene, deren Schriftwechsel richterlicher Kontrolle unterliegt. Daneben sei aber bei allen Gefangenen eine Überwachung des Schriftverkehrs aus Gründen der Behandlung der Gefangenen erforderlich, um Informationen über die Persönlichkeit der Gefangenen zu gewinnen und ggf. Krisensituationen rechtzeitig entgegensteuern zu können. Bei eingehender Behördenpost stehe der Gesichtspunkt der Behandlung der Gefangenen im Vordergrund, da vielfach gerade durch Behördenpost Krisensituationen ausgelöst würden. Darüber hinaus bestehe eine Missbrauchsgefahr, sofern Private ihren Sendungen den Anschein amtlicher Schreiben geben. Aus Verhältnismäßigkeitsgründen beschränke sich die Briefüberwachung bei eingehender Behördenpost auf eine Sichtkontrolle sowie eine Nachschau nach unerlaubten Beilagen. Bei ausgehenden Schreiben an Behörden sei einem Missbrauch durch die Beigabe verschlossener Schreiben an Dritte, die durch die Empfangsbehörden ohne Rückfrage weitergeleitet würden, vorzubeugen. Insgesamt werde dem Grundsatz der Verhältnismäßigkeit durch eine jeweils unterschiedliche Kontrolldichte entsprochen.

Ich sehe jedoch nicht, wie eine vollständige Überwachung des Briefverkehrs in nahezu allen Justizvollzugsanstalten in Bayern dem besonderen Gewicht des Post- und Briefgeheimnisses gerecht wird. Dies gilt vor allem für die Einrichtungen oder Anstalten des offenen Strafvollzuges. Eine Unterbringung im offenen Vollzug kommt gemäß § 10 Abs. 1 Strafvollzugsgesetz ohnehin nur für solche Gefangene in Betracht, die den besonderen Anforderungen dieser Art des Vollzuges genügen. Für sie gilt in besonderem Maße der Grundsatz des § 3 Abs. 1 und 3 Strafvollzugsgesetz, dass der Vollzug darauf auszurichten ist, dem Gefangenen bei seiner Eingliederung in das Leben in Freiheit zu helfen, indem das Leben im Vollzug den allgemeinen Lebensverhältnissen soweit als möglich angeglichen wird. Dadurch soll der Gefangene zu Selbstständigkeit, Eigenverantwortlichkeit und Aktivität befähigt werden. Vor diesem Hintergrund habe ich mehrere Anstalten bzw. Einrichtungen des offenen Strafvollzuges aufgesucht und mich vor Ort über die Praxis der Briefkontrolle informiert. Dabei habe ich festgestellt, das dort die Kontrolle des Schriftwechsels neben der Ordnung der Anstalt in erster Linie auf die Behandlung der Gefangenen gestützt wird. Vor dem Hintergrund des grundrechtlich geschützten Briefgeheimnisses und der damit verbundenen gesetzgeberischen Entscheidung in § 29 Abs. 3 Strafvollzugsgesetz, eine Briefkontrolle nur unter bestimmten Voraussetzungen (soweit erforderlich) zuzulassen, halte ich die generelle, in Bayern offenbar auf allen Ebenen des Vollzuges praktizierte Briefkontrolle für sehr bedenklich. Die Möglichkeit eines kontrollfreien Briefverkehrs ist angesichts der umfassenden Einschränkungen in den meisten bayerischen Justizvollzugsanstalten nicht ersicht-

lich, obwohl das Strafvollzugsgesetz diese Möglichkeit gerade vorsieht. Demgemäß habe ich das Staatsministerium der Justiz um Prüfung gebeten, ob ein besserer Ausgleich zwischen den Bedürfnissen des Strafvollzuges und dem Schutz vor Eingriffen in das Briefgeheimnis der Strafgefangenen gefunden werden kann. Das Justizministerium hat jedoch eine Änderung der bisherigen Praxis abgelehnt.

8.3.2 Einsicht in den Gefangenenpersonalakt

Durch das Vierte Strafvollzugsänderungsgesetz, das seit dem 01.12.1998 in Kraft ist (siehe hierzu auch meinen 17. Tätigkeitsbericht Nr. 7.1.3 und 18. Tätigkeitsbericht Nr. 7.1.4), wurde in § 185 Strafvollzugsgesetz das Recht des Gefangenen auf Auskunft aus „seinem“ Gefangenenpersonalakt bzw. Einsicht in den selben formuliert. Durch mehrere Eingaben habe ich allerdings den Eindruck gewonnen, dass bei der Anwendung dieser Vorschrift noch erhebliche Unsicherheiten bestehen. Im Rahmen meiner Korrespondenz mit dem Staatsministerium der Justiz und mehreren Justizvollzugsanstalten habe ich daher folgende Maßgaben für die Umsetzung des Auskunfts- bzw. Akteneinsichtsrechts herausgestellt:

Grundsätzlich erhält der Gefangene gemäß § 185 Strafvollzugsgesetz und nach Maßgabe des § 19 Bundesdatenschutzgesetz **Auskunft** über die zu seiner Person gespeicherten Daten. Hierfür soll er die Art der personenbezogenen Daten, über die er Auskunft wünscht, näher bezeichnen. Sofern die Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert sind, was für eine Vielzahl der Daten des Justizvollzuges noch der Fall sein wird, ist Voraussetzung für die Auskunftserteilung, dass der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Allerdings dürfen an die vom Betroffenen zu machenden Angaben keine zu hohen Anforderungen gestellt werden. Kann der Betroffene bspw. nur Angaben über die Art der Daten machen, die er aufgrund konkreter Umstände im Gefangenenpersonalakt vermutet, deren genauem Ort in dem Akt er aber gerade nicht kennt und auch nicht kennen kann, so darf ihm in der Regel nicht aufgegeben werden, zusätzliche Konkretisierungen vorzunehmen, die ihm erst nach Erteilung der Auskunft zugänglich sind. Das Erfordernis zusätzlicher Angaben, das der Gesetzgeber eingeführt hat, um den Aufwand der ersuchten Behörde für das Auffinden der Daten gering zu halten, muss mit dem hinter dem Antrag des Betroffenen stehenden Interesse abgewogen werden. Bei der Beurteilung der

Verhältnismäßigkeit des zur Auskunftserteilung erforderlichen Aufwandes muss dabei stets auf den Einzelfall abgestellt werden. Eventuell zu erwartende Anträge weiterer Gefangener dürfen hierbei keine Rolle spielen.

Sofern die Auskunft für die Wahrnehmung der rechtlichen Interessen des Betroffenen nicht ausreicht und er hierfür auf die Einsichtnahme angewiesen ist, erhält er Akteneinsicht. Das Akteneinsichtsersuchen muss dementsprechend ebenfalls die betreffenden Daten sowie zusätzlich die nur durch eine Akteneinsicht wahrnehmbaren rechtlichen Interessen konkret benennen.

Nach Maßgabe des § 19 Abs. 4 Bundesdatenschutzgesetz kann die Auskunft/Akteneinsicht verweigert werden, insbesondere wenn ansonsten die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährdet würde oder die Daten wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.

8.3.3 Besuchskontrolle

Die Überprüfung von Besuchern in Justizvollzugsanstalten und die diesbezüglichen Datenerhebungen sind bereits längerer Zeit Gegenstand einer Korrespondenz zwischen mir und dem Staatsministerium der Justiz (siehe 19. Tätigkeitsbericht Nr. 7.4.2). Rechtsgrundlage für eine derartige Datenerhebung ist § 179 Abs. 3 Strafvollzugsgesetz. Danach können Daten über Besucher zum Zwecke einer Kontrolle nach § 25 Strafvollzugsgesetz auch ohne deren Mitwirkung bei Personen oder Stellen außerhalb der Justizvollzugsanstalt erhoben werden. Das Einverständnis des Besuchers ist dazu nicht erforderlich. Das Staatsministerium der Justiz möchte dennoch an der bisherigen Praxis der Einholung einer Einwilligungserklärung festhalten. Es hat mir allerdings versichert, dass nicht beabsichtigt sei, aufgrund der Einwilligung Daten zu erheben, die von der gesetzlichen Befugnis nicht gedeckt sind.

Im Interesse einer einheitlichen und datenschutzfreundlichen Verfahrensweise hat das Staatsministerium der Justiz ein Formblatt für die Besucherüberprüfung entwickelt. Hierbei wurde ich beteiligt. Dabei habe ich, vorbehaltlich meiner weiterhin bestehenden grundsätzlichen Einwände

gegen die Erholung einer Einwilligunserklärung, darauf Wert gelegt, dass Angaben des Besuchers, die keine zwingende Voraussetzung für eine Zulassung zum Besuch sind, deutlich als freiwillige Angaben gekennzeichnet werden. Auch sollte der Besucher darauf hingewiesen werden, dass eine Überprüfung seiner Person sowie - bei positivem Ergebnis - die Zulassung zum Besuch auch möglich ist, wenn er sich mit seiner Überprüfung nicht einverstanden erklärt. Das Staatsministerium der Justiz ist diesen Anregungen nachgekommen und hat die Justizvollzugsanstalten in Bayern gebeten, bei Bedarf das neu entwickelte einheitliche Formblatt zu verwenden.

8.3.4 Datenübermittlungen an andere Justizvollzugsanstalten

Ein Strafgefangener hatte sich an mich gewandt, weil sein Gefangenenpersonalakt mit samt der darin enthaltenen Begutachtungen und Unterlagen über Schriftverkehr mit Familienmitgliedern von „seiner“ Justizvollzugsanstalt an eine nicht für ihn zuständige Justizvollzugsanstalt übersandt worden war. Hintergrund dieser Datenübermittlung war, dass der Gefangene Briefkontakt mit einer Gefangenen in der anderen Justizvollzugsanstalt hatte und diese Anstalt ihrer Gefangenen diesen Schriftwechsel untersagen wollte, weil sie ansonsten einen schädlichen Einfluss auf sie oder ihre Eingliederung bzw. eine Gefährdung der Sicherheit und Ordnung in der Anstalt befürchtete. Um die Untersagung im gerichtlichen Verfahren zu untermauern, forderte sie den Gefangenenpersonalakt des Eingabeführers an, um zusätzlich zu den bei ihr vorliegenden Erkenntnissen auch diese Unterlagen auszuwerten. Daraufhin wurde ihr der Akt übersandt.

Für eine derartige Datenübermittlung besteht jedoch keine Rechtsgrundlage. Mit dem Vierten Strafvollzugsänderungsgesetz wurde in § 180 Strafvollzugsgesetz eine abschließende Regelung getroffen, unter welchen Voraussetzungen eine Justizvollzugsanstalt Daten über Gefangene an Dritte übermitteln darf. Die dort genannten Voraussetzungen unter denen eine Datenübermittlung zulässig wäre, lagen im Falle des Eingabeführers nicht vor. Dies gilt um so mehr, als das Gesetz der Übermittlung von Erkenntnissen aus der Überwachung des Schriftverkehrs zusätzliche enge Grenzen zieht. Die Übersendung des Gefangenenpersonalaktes kann auch nicht damit gerechtfertigt werden, dass die ersuchende Justizvollzugsanstalt eine Befugnis zur Erhebung der für ihr gerichtliches Verfahren erforderlichen Daten hatte. Diese vom Staatsministerium der Justiz unter Bezugnahme auf gerichtliche Entscheidungen vertretene Auffassung verkennt, dass das Gesetz ausdrücklich zwischen Befugnissen zur Datenerhebung und zur Datenübermittlung unter-

scheidet und dass der Schluss von Erhebungsbefugnissen auf die Übermittlungsbefugnis den sorgfältig formulierten Katalog der Übermittlungsgründe sowie die insbesondere für Erkenntnisse aus der Briefüberwachung zusätzlich aufgestellten Beschränkungen unterlaufen würde. Schließlich können Eingriffe in die Rechte eines Gefangenen nicht allgemein mit den Bedürfnissen des Strafvollzuges sämtlicher Justizvollzugsanstalten sondern nur mit den Erfordernissen des auf seine Person bezogenen Vollzuges der Freiheitsstrafe begründet werden. Ich erwäge daher, sofern eine Änderung dieser Praxis nicht vorgenommen wird, die Vorgehensweise der beteiligten Justizvollzugsanstalten zu beanstanden.

8.3.5 Verarbeitung besonders sensibler Daten

8.3.5.1 Weitergabe ärztlicher Daten

Auch in einer Justizvollzugsanstalt unterliegen die Erkenntnisse des Anstaltsarztes sowie von Ärzten außerhalb des Vollzuges die mit der Untersuchung oder Behandlung eines Gefangenen beauftragt werden, grundsätzlich der in § 203 Abs. 1 Nr. 1 Strafgesetzbuch sanktionierten Schweigepflicht. Im Hinblick auf die besonderen Anforderungen des Vollzuges hat der Gesetzgeber in § 182 Strafvollzugsgesetz jedoch Durchbrechungen dieser Schweigepflicht vorgesehen. Allerdings sind Offenbarungen unter Berücksichtigung des besonders geschützten Vertrauensverhältnisses zwischen dem Arzt und seinen Patienten nur unter besonders engen Voraussetzungen zulässig. In meiner Korrespondenz mit dem Staatsministerium der Justiz habe ich diese Voraussetzungen herausgearbeitet:

- Offenbarungen von Ärzten dürfen unter den eng begrenzten Voraussetzungen des § 182 Abs. 2 Strafvollzugsgesetz nur gegenüber dem **Anstaltsleiter** erfolgen. Eine Offenbarung gegenüber anderen Vollzugsbediensteten ist nur aufgrund einer Entscheidung des Anstaltsleiter zulässig.

- Die Weitergabe so erlangter Daten durch den Anstaltsleiter an die **Aufsichtsbehörde** ist nicht unbeschränkt möglich, sondern ist an die gleichen Voraussetzungen gebunden wie die Weitergabe an den Anstaltsleiter. Das heißt, dass vom Arzt an den Anstaltsleiter übermittelte Daten von diesem nur an die Aufsichtsbehörde weitergegeben werden dürfen, **soweit** dies für die Wahrnehmung von Aufsichtsbefugnissen unerlässlich oder zur Abwehr erheblicher Gefahren für Leib oder Leben des Gefangenen oder Dritter erforderlich ist.

- Offenbarungen des Arztes gegenüber der **Aufsichtsbehörde** sind nicht ausdrücklich geregelt. Wendet man die allgemeinen Vorschriften an, so kommt § 180 Abs. 1 und 3 Strafvollzugsgesetz als Befugnis zur Offenbarung in Betracht. Derartige Übermittlungen unterliegen gemäß § 180 Abs. 10 Strafvollzugsgesetz jedenfalls den besonderen Beschränkungen der Erforderlichkeit bzw. Unerlässlichkeit des § 182 Abs. 2 Strafvollzugsgesetz.

- Bei der Prüfung der „Erforderlichkeit der Offenbarung" ist auch das Gebot der Verhältnismäßigkeit zu beachten. An Stelle der Offenbarung dürfen keine anderen Maßnahmen zur Verfügung stehen, die, bei gleicher Wirksamkeit für den verfolgten Zweck, das Recht des Gefangenen auf informationelle Selbstbestimmung geringer beinträchtigen würden. „Unerlässlichkeit der Offenbarung" liegt nur vor, wenn die Durchbrechung der Schweigepflicht ultima ratio ist. Die Offenbarung ist mithin die letzte Eingriffsmöglichkeit. Im Regelfall dürfte daher die Offenbarung von personenbezogenen Daten aus dem Bereich der ärztlichen Gesundheitsfürsorge an die Aufsichtsbehörde weder erforderlich noch unerlässlich sein.

8.3.5.2 Aufbewahrung in Sonderheften

Im Zusammenhang mit einer an mich gerichteten Eingabe habe ich erfahren, dass ärztliche sowie psychologische oder psychiatrische Gutachten, die im Rahmen des Strafverfahrens erholt wurden, ohne weitere Sicherung in den Gefangenenpersonalakt der Justizvollzugsanstalt übernommen werden. Da derartige Gutachten besonders sensible Daten enthalten, die einer durch die Strafnorm des § 203 Strafgesetzbuch sanktionierten besonderen Schweigepflicht unterliegen, dürfen sie nur unter besonders engen Voraussetzungen weitergegeben werden. Diese besondere Zweckbindung sollte durch organisatorische Maßnahmen abgesichert werden. Ich habe daher das Staatsministerium der Justiz gebeten, zu prüfen, ob diese besonders sensiblen Unterlagen gesondert aufbewahrt werden könnten. Wobei auch weitere Daten von besonderer Sensibilität wie Erkenntnisse aus der Überwachung von Besuch und Schriftverkehr, erkennungsdienstliche Unterlagen sowie personenbezogene Daten Dritter in diese Überlegungen miteinbezogen werden sollten.

Das Staatsministerium der Justiz hat dahingehende Regelungen abgelehnt, da diese vom Gesetzgeber nicht vorgeschrieben seien. Zudem seien alle Bediensteten einer Justizvollzugsanstalt zur Behandlung eines Gefangenen aufgerufen und müssten demgemäß über entsprechende Kenntnisse verfügen. Schließlich sei ein ausreichender Schutz durch die Regelung des § 183 Strafvollzugsgesetz gegeben, der einzelnen Bediensteten den Zugriff auf personenbezogene Daten nur gestattet, soweit dieser zur Erfüllung der ihnen obliegenden Aufgaben erforderlich ist. Ich bin jedoch weiterhin der Auffassung, dass die Sensibilität der von mir genannten Daten eine besondere Sicherung gegen unbefugte Zugriffe bspw. durch eine gesonderte Aufbewahrung erfordert, zumal eine Einsichtnahme durch einzelne Bedienstete in einen Gefangenenpersonalakt in der Regel nicht einmal dokumentiert wird. In diesem Sinne haben die Datenschutzbeauftragten des Bundes und der Länder auch die Schaffung eigenständiger Löschungs- und Vernichtungsfristen für derartige Daten im Rahmen der Überarbeitung der Aufbewahrungsbestimmungen gefordert.

8.3.6 Zugriff auf Gefangenendaten in „ADV-Vollzug“

Über die Entwicklung eines Informationssystems über Gefangenendaten (ADV-Vollzug) habe ich bereits in meinen vorrangegangenen Tätigkeitsberichten (18. Tätigkeitsbericht Nr. 7.2.4, 19. Tätigkeitsbericht Nr. 7.4.5) berichtet. Dieses System standardisiert Verfahrensabläufe in den Justizvollzugsanstalten und erleichtert zudem den Zugriff auf Daten der Gefangenen. Aus diesem Grund habe ich anlässlich der Umstellung bisheriger Papierformulare auf automatisierte Datenverarbeitung im Dezember 2000 eine inhaltliche Überprüfung der neugefassten Mitteilungen an Behörden außerhalb der Anstalt vorgenommen. Dabei habe ich in mehreren Fällen vorgesehene Datenübermittlungen etwa an Sozial- oder Meldebehörden als nicht erforderlich und damit unzulässig kritisiert, woraufhin das Staatsministerium der Justiz entsprechende Änderungen vorgenommen hat.

Anlässlich einer Prüfung einer Justizvollzugsanstalt, in deren Verlauf ich auch die Anwendung des Systems ADV-Vollzug kontrolliert habe, habe ich festgestellt, dass die Zugriffsrechte für bestimmte Aufgabenbereiche wie die Torwache oder einzelne Dienstgruppen nicht individuell sondern für alle dort tätigen Bediensteten einheitlich zugewiesen werden. Durch einen solchen Zugriff über dasselbe Passwort kann allerdings keine individuelle Verantwortlichkeit für einzelne Zugriffe, die sämtlich mit der gleichen Kennung protokolliert werden, festgestellt werden. Die Zuordnung jedes einzelnen Zugriffes zu einem bestimmten Bediensteten dient aber dem Schutz

vor missbräuchlichen Zugriffen auf personenbezogene Daten. Die Justizvollzugsanstalt hat auf meine Forderung nach einer Änderung dieser Praxis jedem Mitglied der Dienstgruppe ein eigenes Passwort zugeteilt. Für die Torwache hat sie hiergegen den ständigen Personalwechsel sowie spezifische Anforderungen der dortigen Dienstverrichtung, die einen zeitgleichen Zugriff beider dort Beschäftigter erfordern, geltend gemacht. Ich habe hierzu darauf hingewiesen, dass bei einem Zugriff beider gleichzeitig in der Torwache beschäftigter Bediensteter über dieselbe Kennung weitere technisch-organisatorische Vorkehrungen gegen einen missbräuchlichen Datenzugriff getroffen werden müssten, etwa dass ein Zugriff über die Torwachenkennung nur von bestimmten Endgeräten aus zugelassen wird.

Im Verlauf derselben Prüfung habe ich festgestellt, dass die im System ADV-Vollzug vorgesehene Rollenzuweisung (siehe 19. Tätigkeitsbericht Nr. 7.4.5) zwischen einzelnen Datenfeldern und der Art der Zugriffsberechtigung hierauf unterscheidet. Eine Beschränkung des Zugriffs auf die Daten nur bestimmter Gefangener ist jedoch systemseitig nicht vorgesehen. Ich habe das Staatsministerium der Justiz daraufhin um Prüfung gebeten, ob die Berechtigungszuweisung für dieses Informationssystem nicht dahingehend abgeändert werden könnte, das jedem Bediensteten der Zugriff nur auf die Daten solcher Gefangener gestattet wird, für die er dienstlich zuständig ist, da eine Berechtigung für darüber hinausgehende Daten nicht erforderlich ist. Etwaige Schwierigkeiten im Hinblick auf die Notwendigkeit eines erweiterten Zugriffes bei Nachtdiensten, gruppenübergreifenden Arbeitsgruppen oder Vertretungsfällen könnten dabei durch die Einrichtung eines für diese Aufgaben jeweils gesonderten Nutzerprofiles umgangen werden. Das Staatsministerium der Justiz hat eine derartige Änderung der Rollenzuweisung abgelehnt, da die hohe Fluktuation bei Gefangenen und Personal sowie die Vielzahl unterschiedlicher Aufgaben der Bediensteten eine häufige Änderung der Berechtigungszuweisungen bzw. eine große Zahl verschiedener Sonderkennungen bedingen würde, die nicht zu bewältigen sei. Im Hinblick auf die vollständige Protokollierung sämtlicher Zugriffe auf die Daten im Verfahren ADV-Vollzug habe ich dies akzeptiert, sofern durch eine entsprechende Dienstanweisung sowie geeignete Stichprobenkontrollen Vorsorge gegen eine zweckfremde Nutzung der Daten getroffen wird.

9 Gemeinden, Städte und Landkreise

9.1 Änderung des Landeswahlgesetzes

Im Berichtszeitraum wurde das Landeswahlgesetz geändert (Gesetz zur Änderung des Landeswahlgesetzes vom 24. Juni 2002, GVBl. S. 242). Aus datenschutzrechtlicher Sicht sind insbesondere folgende Regelungen von Bedeutung:

In Art. 4 wurde die öffentliche Auslegung des Wählerverzeichnisses in Angleichung an das Bundeswahlrecht (vgl. § 17 BWG) durch ein Recht auf Einsichtnahme in das Wählerverzeichnis unter bestimmten Voraussetzungen ersetzt. Jede stimmberechtigte Person hat danach zunächst die Möglichkeit, die Richtigkeit oder Vollständigkeit der zu ihrer Person im Wählerverzeichnis eingetragenen Daten zu überprüfen. Zur Überprüfung der Richtigkeit oder Vollständigkeit der Daten von anderen im Wählerverzeichnis eingetragenen Personen haben Stimmberechtigte darüber hinaus nur dann ein Recht auf Einsicht in das Wählerverzeichnis, wenn sie Tatsachen glaubhaft machen, aus denen sich eine Unrichtigkeit oder Unvollständigkeit des Wählerverzeichnisses ergeben kann. Das Recht zur Überprüfung besteht nicht hinsichtlich der Daten von Stimmberechtigten, für die im Melderegister ein Sperrvermerk gemäß Art. 34 Abs. 5 MeldeG eingetragen ist; solche Daten werden schon bisher nach § 18 Abs. 2 Satz 2 LWO nicht öffentlich ausgelegt.

Die unbeschränkte Möglichkeit zur Einsichtnahme in das Wählerverzeichnis war nach meinem Dafürhalten nicht mit dem Recht des Bürgers auf informationelle Selbstbestimmung vereinbar. Der Verzicht auf die öffentliche Auslegung des Wählerverzeichnisses wurde deshalb bereits seit längerem von mir gefordert (vgl. 19. TB Nr. 8.2). Damit wurde auch der Tatsache Rechnung getragen, dass in der Vergangenheit von der Möglichkeit der Einsichtnahme in das Wählerverzeichnis in der Praxis kaum Gebrauch gemacht wurde.

In Art. 7 Abs. 4 wird für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Stimmberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen eine Rechtsgrundlage im Landeswahlgesetz geschaffen. Die Verarbeitung und Nutzung der Daten für künftige Abstimmungen ist aber nur zulässig, wenn die Betroffenen dem nach einer Unterrichtung

über ihr Widerspruchsrecht nicht widersprochen haben. Die zulässiger Weise zu erhebenden und zu verarbeitenden Daten werden im Gesetz nunmehr abschließend aufgeführt.

Art. 7 Abs. 5 enthält eine Rechtsgrundlage für die Übermittlung personenbezogener Daten von Bediensteten bayerischer Behörden an die Gemeinden zur Bildung von Wahlvorständen. Die Datenübermittlung setzt ein entsprechendes Ersuchen der Gemeinde an die betreffende Behörde voraus. Die zu übermittelnden Daten sind dabei ebenfalls bereichsspezifisch abschließend aufgezählt. Die ersuchte Stelle hat die Betroffenen über die übermittelten Daten und den Empfänger zu benachrichtigen.

9.2 Einsichtnahme in Wählerverzeichnisse

Im Rahmen der Kommunalwahlen 2002 habe ich vor der Stichwahl am 17.03.2002 einen Hinweis erhalten, es habe möglicherweise unzulässige Einsichtnahmen in Wählerverzeichnisse einer Stadt oder einen entsprechenden Versuch gegeben. Zwar hat sich der Vorgang, über den in den Medien umfassend berichtet wurde, nicht bestätigt. Ich nehme ihn jedoch zum Anlass darauf hinzuweisen, dass Wählerverzeichnisse nur zur Feststellung der Wahlberechtigung, zur Verhinderung einer mehrfachen Stimmabgabe und im Rahmen des Art. 101 Abs. 2 GLKrWO genutzt werden dürfen. Nach § 101 Abs. 1 GLKrWO sind sie so zu verwahren, dass sie gegen Einsichtnahme durch Unbefugte geschützt sind. Auskünfte aus Wählerverzeichnissen dürfen nach Art. 101 Abs. 2 GLKrWO nur Behörden, Gerichten und sonstigen amtlichen Stellen und nur dann erteilt werden, wenn sie für den Empfänger im Zusammenhang mit der Abstimmung erforderlich sind. Ein solcher Anlass liegt insbesondere bei Verdacht von Wahlstraftaten, bei Wahlprüfungsangelegenheiten und bei wahlstatistischen Arbeiten vor. Nach §102 Abs. 2 GLKrWO sind Wählerverzeichnisse nach Ablauf von sechs Monaten seit der Abstimmung zu vernichten, wenn nicht die Rechtsaufsichtsbehörde mit Rücksicht auf ein schwebendes Verfahren über die Wahlanfechtung, Berichtigung oder Ungültigerklärung der Wahl etwas anderes anordnet oder sie für die Strafverfolgungsbehörde zur Ermittlung einer Wahlstraftat von Bedeutung sein können.

9.3 Beantragung eines Wahlscheins in elektronischer Form

Nach § 27 Abs. 1 Satz 2 der Bundeswahlordnung kann die Beantragung von Wahlscheinen für die Bundestagswahlen nun auch per E-Mail oder durch sonstige dokumentierbare Übermittlung

in elektronischer Form (z.B. Antragstellung per Internet-Formular) erfolgen. Das Bayerische Staatsministerium des Innern teilte mir auf Anfrage mit, dass es die Antragstellung auf Erteilung von Wahlscheinen per E-Mail oder durch sonstige Übermittlung in elektronischer Form nicht von besonderen Anforderungen, wie z. B. digitale Signatur, Verschlüsselung o. ä., abhängig machen will. Dies sei trotz der Risiken nicht erforderlich, da der Antrag per E-Mail bzw. per Internet nur eine weitere Möglichkeit der Beantragung des Wahlscheines für den Wahlberechtigten darstellte. Da die Risiken der elektronischen Kommunikation allgemein bekannt seien, müsse es dem Wahlberechtigten selbst überlassen werden, ob er für die Antragstellung ein elektronisches Kommunikationsmittel (also eine Art „offene Postkarte“) verwenden wolle oder ob er eine Antragstellung auf dem herkömmlichen Weg per Post bzw. eine persönliche Antragstellung bevorzuge.

Aus datenschutzrechtlicher Sicht habe ich gegen die Nutzung der modernen Informations- und Kommunikationsmittel (E-Mail oder sonstige dokumentierbare Übermittlungen in elektronischer Form) bei der Wahlscheinbeantragung keine grundsätzlichen Bedenken. Die Kommunen sollten allerdings, sofern sie dem Wahlberechtigten die Nutzung der modernen Informations- und Kommunikationsmittel bei der Wahlscheinbeantragung anbieten wollen, ausdrücklich auf ihrer eigenen Homepage darauf hinweisen, dass die Methoden zur Übermittlung von Daten über das Internet nicht als sicher betrachtet werden können. Ich habe beim Bayerischen Staatsministerium des Innern daher angeregt, die Kommunen in geeigneter Form (z. B. per Verwaltungsvorschrift oder Rundschreiben) darüber zu unterrichten, dass der Bürger auf die Gefahren bei der Nutzung moderner Kommunikationsmittel hinzuweisen ist.

Insbesondere zu der Alternative „Antragstellung per Internet-Formular“ habe ich das Bayerische Staatsministerium des Innern des Weiteren außerdem darauf hingewiesen, dass gemäß § 4 Abs. 4 Ziffer 3 Teledienstedatenschutzgesetz (TDDSG) der Diensteanbieter, hier die betreffende Kommune, durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass „der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann“. Dies lässt sich nur durch die Verwendung geeigneter Verschlüsselungsmethoden sicherstellen. Bei „Internet-Formularen“ bedeutet dies derzeit die Verwendung von SSL-Verschlüsselung. Eine unverschlüsselte Übertragung kann somit (grundsätzlich) nur akzeptiert werden, sofern der Nutzer über die Risiken umfassend informiert wurde und ihm Alternativen (hier: Postversand) angeboten werden. Ich habe beim Bayerischen Staatsministerium des Innern angeregt, dass es darauf hinwirkt,

dass von den Kommunen für das Übertragen der Wahlscheinanträge mittels „Internet-Formular“

- zunächst standardmäßig SSL-Verschlüsslung (SSL v3 mit 128 Bit) eingesetzt wird,

- als zweite Option eine unverschlüsselte Übertragung angeboten wird - nach einer umfassenden Information über die Risiken und nach gezielter Auswahl des Nutzers evtl. mit erneutem Hinweis auf die damit verbundenen Risiken und erzwungener Bestätigung der Kenntnisnahme durch den Nutzer vor dem eigentlichen Absenden des Antrags - und

- als dritte Option auf die postalische Übersendungsmöglichkeit hingewiesen wird.

Diese nach TDDSG zwingend erforderlichen Informationen können technisch z. B. in einem Informationsfenster mit den entsprechenden Auswahlmöglichkeiten der vom Nutzer bevorzugten Option ohne weiteres realisiert werden. Auch die Verwendung von SSL auf dem jeweiligen Web-Server ist heutiger Stand der Technik und ohne großen Aufwand realisierbar.

Das Bayerische Staatsministerium des Innern hat auf meine oben genannten Anregungen hin die Kommunen in einem Rundschreiben entsprechend unterrichtet.

9.4 Veröffentlichung von Sitzungsvorlagen im Internet

Eine Gemeinde hat mich gebeten zu prüfen, ob gegen eine Veröffentlichung von Sitzungsvorlagen für öffentliche Sitzungen der gemeindlichen Gremien im Internet datenschutzrechtliche Bedenken bestehen. Ich vertrete dazu folgende Auffassung:

Bei einer Veröffentlichung von Sitzungsvorlagen im Internet bestehen die gleichen Gefahren wie bei einer Veröffentlichung von Sitzungsniederschriften. Dies sind insbesondere die Möglichkeit einer weltweit automatisierten Auswertung der Veröffentlichung nach verschiedenen Suchkriterien, die beliebig miteinander verknüpft werden können, sowie die internetspezifischen Gefahren für die Datensicherheit. Im Einzelnen verweise ich dazu auf meinen Betrag im 18. Tätigkeitsbericht unter der Nr. 8.9 zur Veröffentlichung von Niederschriften über öffentliche Sitzungen des Gemeinderats im Internet und auf den Kommentar zum BayDSG, Wilde/Ehmann/Niese/Knoblauch, Handbuch XII.8a).

Sitzungsvorlagen für öffentliche Sitzungen gemeindlicher Gremien sind **interne** Ausarbeitungen der Verwaltung für den Gemeinderat bzw. den Ausschuss. Soweit sie personenbezogene Daten enthalten kommt aus datenschutzrechtlicher Sicht eine Weitergabe an Dritte (hier weltweit an eine Vielzahl unbestimmter Personen) mangels einer bereichsspezifischen Regelung nur unter den Voraussetzungen des Art. 19 Abs. 1 des Bayerischen Datenschutzgesetzes (BayDSG) in Betracht.

Nach Art. 19 Abs. 1 Nr. 1 BayDSG setzt die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen u. a. voraus, dass sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Sitzungsvorlagen sind wie gesagt Ausarbeitungen der Gemeindeverwaltung, die im Rahmen der Vorbereitung der Beratungsgegenstände durch den ersten Bürgermeister gemäß Art. 46 Abs. 2 Satz 1 GO den Gemeinderatsmitgliedern zur internen Information zur Verfügung gestellt werden. Zur Information der Gemeinderatsmitglieder ist eine Veröffentlichung der Sitzungsvorlagen im Internet nicht erforderlich. Da eine derartige Datenübermittlung somit zur Aufgabenerfüllung der Gemeinde nicht erforderlich ist, scheidet Art. 19 Abs. 1 Nr. 1 BayDSG als Rechtsgrundlage aus.

Nach Art. 19 Abs. 1 Nr. 2 BayDSG ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein berechtigtes Interesse der Öffentlichkeit an der Kenntnis interner Sitzungsunterlagen mit personenbezogenem Inhalt besteht nicht. Außerdem müssen die Bürger grundsätzlich darauf vertrauen können, dass mit ihrer Angelegenheit nur die zuständigen Stellen befasst werden und der Vorgang im internen Verhältnis Bürger-Verwaltung-Entscheidungsgremium verbleibt.

Aus **datenschutzrechtlicher Sicht** ist eine Veröffentlichung von Sitzungsvorlagen im Internet daher nur dann zulässig, wenn diese durch Kürzen, Schwärzen etc. so abgeändert werden, dass sie nur noch Informationen enthalten, die ohne Bedenken der Öffentlichkeit zugänglich gemacht werden dürfen. Da jedoch auch bei einer Veröffentlichung derart „bereinigter“ Sitzungsvorlagen die vom Staatsministerium des Innern unten unter der Nr. 3 dargestellten Probleme bestehen, muss auch aus datenschutzrechtlicher Sicht generell von einer Veröffentlichung von Sitzungsvorlagen im Internet abgeraten werden.

Das Staatsministerium des Innern, das ich in der Angelegenheit um Stellungnahme gebeten habe, teilte dazu aus kommunalrechtlicher Sicht Folgendes mit:

1. Zunächst weist auch das Innenministerium darauf hin, dass es sich bei den Sitzungsvorlagen grundsätzlich um Ausarbeitungen handelt, die zur **internen** Information der Gemeinderatsmitglieder bestimmt sind.

   Ferner gibt es zu bedenken, dass auch bei den Sitzungsvorlagen für öffentliche Sitzungen geheimhaltungsbedürftige Angelegenheiten im Sinne des Art. 20 Abs. 2 Satz 1 GO enthalten sein können.

2. Eine Veröffentlichung der Sitzungsvorlagen ist nach Auffassung des Ministeriums daher allenfalls dann zulässig, wenn sowohl der Bürgermeister als auch der Gemeinderat der Veröffentlichung zugestimmt haben und in den Sitzungsvorlagen nur Tatsachen enthalten sind, die entweder offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die Sitzungsunterlagen müssten daher jeweils **individuell** auf ihre Veröffentlichungsfähigkeit überprüft werden. Gegebenenfalls müssten sie durch Kürzen und Schwärzen so abgeändert werden, bis sie nur noch die Informationen enthalten, die ohne Bedenken der Öffentlichkeit zugänglich gemacht werden können.

   Dies gelte insbesondere für Sitzungsvorlagen, in denen personenbezogene Daten enthalten sind. Der Landesbeauftragte für den Datenschutz führe in seinem 19. Datenschutzbericht (Nr. 8.9) zu Recht aus, dass ein Bürger grundsätzlich darauf vertrauen können muss, dass mit seinem Anliegen nur die zuständigen Stellen befasst werden und sein Schreiben im internen Verhältnis Bürger-Verwaltung-Entscheidungsgremium verbleibt. Es könne nicht ohne Weiteres davon ausgegangen werden, dass der Bürger damit einverstanden ist, dass seine Formulierungen im Einzelnen in vollem Umfang der Öffentlichkeit zur Verfügung gestellt werden.

   Eine Geheimhaltungsbedürftigkeit könne sich zum Beispiel aber auch daraus ergeben, dass der Gemeinde aus der Veröffentlichung taktischer Überlegungen ein Schaden entstehen könnte (z. B. Kaufpreisüberlegungen).

3. Aber auch die Veröffentlichung derart „bereinigter“ Sitzungsvorlagen wirft nach Auffassung des Innenministeriums folgende grundsätzliche Probleme auf:

   a) Die unter Nr. 2 gemachten Ausführungen zeigten, dass es eines hohen Verwaltungsaufwandes bedarf, um sämtliche Sitzungsvorlagen so zu „bereinigen“, dass sie der Öffentlichkeit zugänglich gemacht werden können. Dabei steigt auch - je umfangreicher eine Sitzungsvorlage ist - das Risiko, dass geheimhaltungsbedürftige Angelegenheiten aus Versehen veröffentlicht werden.

   b) Um den hohen Verwaltungsaufwand, den eine Veröffentlichung der Sitzungsvorlagen im Internet bedeutet, zu verringern und um das Risiko der Veröffentlichung geheimhaltungsbedürftiger Angelegenheiten zu vermeiden, werden die Sitzungsvorlagen für den Gemeinderat in der Praxis voraussichtlich in Umfang und Inhalt erheblich reduziert werden. Darunter würde aber die Qualität der vorherigen Information der Mitglieder des Gemeinderats sowie deren Möglichkeit, sich auf die jeweiligen Tagesordnungspunkte vorzubereiten, leiden.

   c) Werden die Sitzungsvorlagen vor der Sitzung im Internet veröffentlicht, wird die Diskussion zu den Tagesordnungspunkten in der Öffentlichkeit auch bereits vor der betreffenden Gemeinderatssitzung anhand der Sitzungsvorlagen geführt werden. Dadurch steigt die Gefahr, dass die öffentliche Meinung bereits in hohem Maße durch die Medien detailliert festgelegt wird und eine freie, ungezwungene Beratung und Beschlussfassung im Gemeinderat erheblich erschwert wird.

   d) Bei einer Veröffentlichung im Internet könnten die eingestellten Informationen weltweit abgerufen und elektronisch ausgewertet werden (Erstellung von „Profilen“). Darüber hinaus könne nicht sichergestellt werden, dass der Bürger jederzeit auf vollständige und unverfälschte Sitzungsvorlagen zugreifen kann (vgl. insoweit auch Nr. 8.9 des 18. Datenschutzberichts). In diesem Zusammenhang könnten sich für die Gemeinde unter Umständen auch haftungsrechtliche Folgen ergeben.

Auch aus Sicht des Innenministeriums ist eine Veröffentlichung der Sitzungsvorlagen im Internet daher zwar grundsätzlich rechtlich nicht unzulässig, wenn die oben erwähnten Vorgaben beachtet werden, von einer Veröffentlichung rät jedoch auch das Ministerium ab.

9.5 Meldung einer öffentlichen Musikveranstaltung gemäß Art. 19 LStVG an die GEMA

Durch eine Eingabe bin ich darauf aufmerksam gemacht worden, dass verschiedene Gemeinden Abdrucke sicherheitsrechtlicher Anzeigen öffentlicher Veranstaltungen (nach Art. 19 Landesstraf- und Versordnungsgesetz - LStVG) an die Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) weiterleiten. Das geschieht, wenn der Anzeigende folgende Formulierung auf dem Formular, auf dem er seine Angaben zu der Veranstaltung macht, durch seine Unterschrift mit abgedeckt hat: „Ein Abdruck ist als Aufführungsmeldung an die GEMA weiterzuleiten." Ich vertrete dazu folgende Auffassung:

Da es für die Übermittlung der Daten aus der Anzeige nach Art. 19 LStVG von der Gemeinde an die GEMA keine Rechtsgrundlage gibt, ist die Weitergabe der Daten gemäß Art. 15 Abs. 1 Nr. 2 BayDSG nur zulässig, wenn der Anzeigende hierzu seine rechtswirksame Einwilligung erklärt hat. Die zitierte Formulierung auf den Anzeigenvordrucken entspricht nicht den datenschutzrechtlichen Anforderungen an eine rechtswirksame Einwilligung, da der Einwilligende vorher nicht ausreichend über die Tragweite seiner Einwilligung informiert wird. Die konkrete Situierung der Formulierung „ein Abdruck ist als Aufführungsmeldung an die GEMA weiterzuleiten" mit dem Feld „Ort und Tag" neben der Unterschrift des Veranstalters ist durchaus missverständlich. Diese Vordruckgestaltung kann bei dem Unterschreibenden auch den Eindruck auslösen, dass die Weiterleitung an die GEMA sich aus einer vorgegebenen Verpflichtung ergibt, und das freie Feld „Ort und Tag" sich auf Ort und Tag der Anmeldung nach Art. 19 LStVG bezieht. Es ist durchaus nicht gesichert, dass jedem klar ist, dass er mit dem Ausfüllen des freien Feldes „Ort und Tag" und der Unterschrift gleichzeitig sein freies Einverständnis zur Weiterleitung der Aufführungsmeldung an die GEMA geben soll.

Wenn überhaupt an einer Einverständniserklärung in dem Anmeldeformular festgehalten werden soll, so müsste die Erklärung klar und unmissverständlich dahin gehend formuliert werden, dass keine öffentlich-rechtliche Verpflichtung zur Abgabe dieser Erklärung besteht (etwa durch den Satz „Ich bin damit einverstanden, dass die Gemeinde für eine Anmeldung meiner Veranstaltung bei der GEMA einen Abdruck dieser Anzeige an die GEMA weiterleitet" und durch die Aufnahme von Ja/Nein-Feldern, mit deren Ankreuzung dieser Wille unmissverständlich kundgetan wird), weiter müsste die Einwilligungserklärung deutlich im Text (z. B. durch Fettdruck, großer

Schrifttyp oder Umrahmung des Textes) hervorgehoben werden. Die Vordrucke wären so zu gestalten, dass die für die GEMA nicht erforderlichen Daten, z. B. die Kostenentscheidung der Gemeinde, nicht weitergeleitet werden.

Zulässig wäre nach meiner Auffassung auch ein Verfahren, bei dem die Gemeinden für die Veranstalter lediglich die von der GEMA zur Verfügung gestellten Anmeldevordrucke als Service auslegen, ohne weiteren Einfluss auf die Anmeldung bei der GEMA zu nehmen.

Das Bayerische Staatsministerium des Innern teilt meine Auffassung. In einem Rundschreiben an die Regierungen hat es auf die Anforderungen hingewiesen, die beachtet werden müssen, wenn das Anmeldeformular eine Einverständniserklärung zur Datenweitergabe beinhalten soll. Alternativ ist auch nach Auffassung des Ministeriums eine freiwillige Bereithaltung von gesonderten GEMA-Anmeldevordrucken bei den Gemeinden denkbar.

9.6 Veröffentlichung von Daten über die Eheschließung

Bürger haben sich bei mir über die Rechtslage bei der Veröffentlichung von Daten über Eheschließungen durch die Gemeinde im gemeindlichen Mitteilungsblatt bzw. im Internet erkundigt. Ich habe ihnen Folgendes mitgeteilt:

Die Veröffentlichung von Eheschließungen stellt eine Datenübermittlung im Sinne von Art. 4 Abs. 6 Satz 2 Nr. 3 Bayerisches Datenschutzgesetz (BayDSG) dar. Sie ist nur zulässig, wenn sie durch eine Rechtsvorschrift erlaubt oder angeordnet wird oder wenn der Betroffene darin eingewilligt hat (Art. 15 Abs. 1 BayDSG).

Mit dem Gesetz zur Neuordnung des Eheschließungsrechts vom 04.05.1998 (EheschlRG) wurden eine Reihe von Vorschriften bezüglich der Eheschließung geändert. Unter anderem wurde das sog. Aufgebot abgeschafft, dessen öffentlicher Aushang nicht länger erforderlich und datenschutzrechtlich bedenklich war. Nach derzeit geltendem Recht haben die Verlobten die beabsichtigte Eheschließung lediglich bei dem für die Eheschließung zuständigen Standesbeamten anzumelden (vgl. §§ 4, 6 Personenstandsgesetz).

Sowohl nach personenstands- als auch nach datenschutzrechtlichen Bestimmungen ist es nur dann möglich, Informationen über Eheschließungen an die Presse weiterzugeben, sofern die betroffenen Bürger nach genauer Information sich mit der Weitergabe ihrer Daten einverstanden erklärt haben. Auch die Bekanntgabe von Eheschließungen im gemeindlichen Mitteilungsblatt darf, mangels einer Rechtsvorschrift, die dies erlauben oder anordnen würde, nur mit Einwilligung der Betroffenen erfolgen. Dazu genügt nicht, dass die Verlobten der Veröffentlichung nicht widersprochen haben, sondern dass sie gegenüber der Gemeinde ihr Einverständnis hierzu erklärt haben. Dies gilt auch bei einer Veröffentlichung dieser Daten im Internet auf der Homepage der jeweiligen Gemeinde.

9.7 Datenschutz in Planfeststellungsverfahren

Im 17. Tätigkeitsbericht habe ich mich unter der Nr. 8.14 zu Fragen der Behandlung personenbezogener Daten in Planfeststellungsverfahren geäußert. In dem Beitrag habe ich u. a. auf Entscheidungen des Bundesverfassungsgerichts hingewiesen, in denen das Gericht die Veröffentlichung von personenbezogenen Daten, die ein Einwendungsführer der Planfeststellungsbehörde preis gibt, um ihr eine sachgerechte Beurteilung der geltend gemachten Einwendungen zu ermöglichen, für verfassungswidrig erklärt. Das Bundesverfassungsgericht hat darauf hingewiesen, dass keine Gründe ersichtlich seien, warum eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses notwendig voraussetze, dass sachbezogene Erwägungen zur Beurteilung und Gewichtung der geltend gemachten Einwendungen personenbezogen in die Begründung aufgenommen und mit dieser veröffentlicht werden müssten. Die sachliche Zuordnung könne hier auch durch die Vergabe von Betriebsnummern erfolgen.

Im Berichtszeitraum hat sich ein Bürger bei mir darüber beschwert, dass eine Regierung in einem Planfeststellungsbeschluss für ein Straßenbauvorhaben personenbezogene Daten, die er als Einwendungsführer im Verfahren der Planfeststellungsbehörde preisgegeben hatte, veröffentlicht hat. Der Planfeststellungsbeschluss enthielt unter namentlicher Nennung des Petenten und seiner Adresse Ausführungen zu seinen wirtschaftlichen Verhältnissen.

Die personenbezogene Abhandlung der Einwendungen des Petenten im Planfeststellungsbeschluss stellte einen rechtswidrigen Eingriff in dessen Recht auf informationelle Selbstbestimmung dar. Den Datenschutzverstoß habe ich beanstandet. In kurz darauf erschienenen Zeitungs-

berichten über den Vorgang wurde mitgeteilt, dass die beanstandete Regierung die betroffenen Bürger künftig nicht mehr beim Namen nennen, sondern deren Einwendungen verschlüsseln will. Ähnlich werde es in den anderen Regierungsbezirken bereits gehandhabt. Nach Angaben des Innenministeriums in den Zeitungsartikeln werden personenbezogene Daten in Planfeststellungsbeschlüssen mittlerweile überall vertraulich behandelt.

9.8 Vorschlagsliste für die Wahl der ehrenamtlichen Richter für das Verwaltungsgericht

Ein Abgeordneter hat mich gebeten zu prüfen, ob den Mitgliedern des Kreistags in den Unterlagen zur Vorbereitung auf die Kreistagssitzung, in der die in die Vorschlagsliste für ehrenamtliche Richter nach § 28 der Verwaltungsgerichtsordnung aufzunehmenden Personen bestimmt werden, das Geburtsdatum und der Beruf der Kandidaten für die Vorschlagsliste mitgeteilt werden dürfen. Ich vertrete dazu folgende Auffassung:

Ich halte diese Angaben für datenschutzrechtlich zulässig, da sie als sachgerechte Prüfkriterien für eine entsprechende Entscheidung anzusehen sind.

Erfolgt die Sitzungsvorbereitung wie im vorliegenden Fall auch durch die Versendung von Sitzungsunterlagen, hätte ich aus datenschutzrechtlicher Sicht auch keine grundsätzlichen Bedenken gegen die Mitteilung des Geburtsdatums und des Berufs der Kandidaten für die Vorschlagsliste nach § 28 der Verwaltungsgerichtsordnung auf den versandten Wahlzetteln, sofern in der Vergangenheit keine personenbezogenen Daten an die Öffentlichkeit gelangt sind, die in übersandten Sitzungsunterlagen enthalten waren. Ich empfehle jedoch, die übersandten Unterlagen mit personenbezogenen Angaben der Kandidaten nach der Behandlung der Angelegenheit im Kreistag wieder einzusammeln und die Mandatsträger zu verpflichten, keine Kopien davon anzufertigen. Dies halte ich insbesondere zum Schutz des Rechts auf informationelle Selbstbestimmung der Kandidaten für erforderlich, die letztlich nicht in die Vorschlagsliste aufgenommen werden.

9.9 Einsichtnahme in kommunale Archivakten

Im Berichtszeitraum habe ich mehrere Anfragen von Heimatforschern zu den Voraussetzungen einer Einsichtnahme in kommunale Archivakten erhalten. Aus datenschutzrechtlicher Sicht vertrete ich dazu folgende Auffassung:

Gemeindeverwaltungen und andere öffentliche Stellen müssen bei der Herausgabe personenbezogener Daten die dafür einschlägigen gesetzlichen Bestimmungen beachten. Mit der Übergabe von Unterlagen an ein Archiv treten die bereichsspezifischen Vorschriften des BayArchivG über die Benützung des Archivguts an die Stelle der allgemeinen Vorschriften des BayDSG (Art. 2 Abs. 7 BayDSG).

Soweit personenbezogene Unterlagen eingesehen werden sollen, die sich im Gemeindearchiv befinden, ist bei der Entscheidung über die Zulässigkeit der Nutzung die von der Gemeinde erlassene Benutzungsordnung oder Benutzungssatzung zu berücksichtigen.

Für personenbezogene Daten einschließlich datenschutzrechtlich gesperrter Daten ist Art. 13 Abs. 2 BayArchivG anzuwenden. Danach gelten auch für die Benützung kommunaler Archive die Vorschriften zum Schutz des Persönlichkeitsrechts des Betroffenen der Art. 10 Abs. 2 Sätze 1 bis 3 Nrn. 1 bis 3, Abs. 3 Sätze 2 bis 6, Abs. 4 und Abs. 5 BayArchivG sinngemäß. Archivgut kann benützt werden, soweit ein berechtigtes Interesse an der Benützung glaubhaft gemacht wird und Schutzfristen nicht entgegenstehen (Art. 10 Abs. 2 Satz 1 BayArchivG).

Grundsätzlich kann jeder Archivgut benützen, der ein von der Rechtsordnung gebilligtes Interesse daran hat. Ein berechtigtes Interesse liegt u. a. vor, wenn die Einsichtnahme zu wissenschaftlichen bzw. heimatkundlichen Zwecken erfolgt (Art. 10 Abs. 2 Satz 2 BayArchivG). Die Benützung ist allerdings zu versagen und kann mit Auflagen versehen werden, wenn Grund zu der Annahme besteht, dass schutzwürdige Belange des Betroffenen oder Dritter entgegenstehen (Art. 10 Abs. 2 Satz 3 Nr. 2 BayArchivG).

Voraussetzung für die Benützung von Archivgut ist der Ablauf von Schutzfristen, die in Art. 10 Abs. 3 BayArchivG im Einzelnen geregelt sind. Archivgut, das sich auf natürliche Personen be-

zieht, darf erst 10 Jahre nach dem Tod des Betroffenen eingesehen werden; ist der Todestag nicht oder nur mit unvertretbarem Aufwand festzustellen, endet die Schutzfrist 90 Jahre nach der Geburt des Betroffenen (Art. 10 Abs. 3 Satz 2 und 3 BayArchivG). Maßgeblich ist die längste Schutzfrist, die auf das jeweilige Archivgut anzuwenden ist. Bei Archivgut, das sich auf natürliche Personen bezieht, können die Schutzfristen nur unter den engen Voraussetzungen des Art. 10 Abs. 4 Satz 2 BayArchivG verkürzt werden. Für Archivgut, das dem Steuergeheimnis, dem Sozialgeheimnis oder sonstigen Rechtsvorschriften des Bundes über Geheimhaltung unterliegt, gilt die Schutzfrist des Bundesarchivgesetzes (Art. 10 Abs. 3 Satz 5 BayArchivG).

Soweit personenbezogene Unterlagen eingesehen werden sollen, die sich nicht im Archiv befinden, gelten die einschlägigen bereichsspezifischen Vorschriften:

Wird eine Einsichtnahme in Personenstandsbücher gewünscht, unterliegt diese den Voraussetzungen des § 61 Personenstandsgesetz. In diesem Zusammenhang weise ich darauf hin, dass Personenstandsbücher nicht an Archive abgegeben werden dürfen. Das Bayerische Archivgesetz ist somit nicht anwendbar.

Eine Offenbarung von Steuergeheimnissen ist nach § 30 Abs. 4 Nr. 3 der Abgabenordnung nur mit Zustimmung der betroffenen Steuerpflichtigen zulässig.

Personenbezogene Daten aus dem Melderegister dürfen nur im Rahmen der melderechtlichen Vorschriften eingesehen werden. Auskünfte über Daten aus dem Melderegister an Private dürfen erteilt werden, wenn dies nach Art. 34 MeldeG zulässig ist. Im Zusammenhang mit der Nutzung der Daten des Melderegisters über verstorbene oder weggezogene Einwohner ist insbesondere die Löschungspflicht des Art. 11 MeldeG zu beachten. Die Meldebehörde kann in den in Art. 12 Abs. 1 genannten Fällen nicht mehr erforderliche Unterlagen an das Gemeindearchiv abgeben, soweit dort ausreichende Datenschutzmaßnahmen getroffen sind.

Eine zusammenfassende Darstellung, welche datenschutzrechtlichen Bestimmungen für die Gemeinden gelten, wenn sie um Mithilfe bei der Erstellung von Ortschroniken, Heimatbüchern oder ähnlichen Werken gebeten werden, enthält eine Veröffentlichung von Knoblauch in der Kommunalpraxis Nr. 10/1996, S. 335 ff. Außerdem verweise ich auf die umfassenden Ausführungen zum Datenschutz im Archivwesen von Wilde/Ehmann/Niese/Knoblauch, Kommentar zum BayDSG, Handbuch XVI.

9.10 Verwendung der Blind-Copy-Funktion oder von Einzelanschriften beim Versand von Antwortschreiben per E-Mail an mehrere Empfänger

Eine Gemeinde hat beim Versand von Antwortschreiben per E-Mail an mehrere Eingabeführer, die sich in der gleichen Angelegenheit an die Gemeinde gewandt hatten, jedem Empfänger die E-Mail-Adresse aller anderen Eingabeführer bekannt gegeben. Damit wurde jedem Eingabeführer mitgeteilt, wer sich außer ihm in der Angelegenheit an die Gemeinde gewandt hatte. Einige der Betroffenen haben sich daraufhin an mich gewandt. Ich weise dazu auf Folgendes hin:

Die Weitergabe der E-Mail-Adressen der anderen Eingabeführer an jeden einzelnen Petenten waren Datenübermittlungen an nicht-öffentliche Stellen. Die Datenübermittlungen hätten durch die Verwendung der Blind-Copy-Funktion oder durch Einzelanschriften vermieden werden können. Sie waren somit zur Beantwortung der Eingaben nicht erforderlich. Die Eingabeführer hatten auch kein berechtigtes Interesse an der Kenntnis, wer sich außer ihnen in der Angelegenheit an die Gemeinde gewandt hatte. Mangels Vorliegen der Voraussetzungen des Art. 19 Abs. 1 des Bayerischen Datenschutzgesetzes (BayDSG) waren die Datenübermittlungen damit unzulässig.

Von einer Beanstandung des Datenschutzverstoßes habe ich für dieses Mal nach Art. 31 Abs. 3 BayDSG abgesehen, nachdem mir die Gemeinde mitgeteilt hat, dass sie die E-Mail-Teilnehmer der Gemeindeverwaltung ausdrücklich darauf hinweisen wird, darauf zu achten, dass bei einer Verwendung an mehrere Empfänger der jeweilige Empfänger nur seine eigene E-Mail-Adresse mitgeteilt bekommt.

10 Einwohnermeldewesen

10.1 Änderung des Melderechtsrahmengesetzes

Am 03.04.2002 ist das Gesetz zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze vom 25.03.2002 in Kraft getreten (BGBl. I S. 1186). Es enthält in seinem Artikel 1 die dritte

und bisher umfassendste Änderung des Melderechtsrahmengesetzes (MRRG) mit der die erforderlichen Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechnologien geschaffen sowie unnötige Meldepflichten abgeschafft werden sollen. Weitere Änderungen betreffen die Schutzrechte der Betroffenen und die Melderegisterauskünfte. Aus datenschutzrechtlicher Sicht sind insbesondere folgende Neuregelungen von besonderer Bedeutung:

In § 7 im MRRG werden die Schutzrechte des Betroffenen zusammengefasst. Durch die Einführung der Gebühren- und Kostenfreiheit für die Inanspruchnahme dieser Rechte soll die datenschutzrechtliche Situation des Einzelnen verbessert werden.

§ 8 MRRG regelt die Auskunft an den Betroffenen. Nach der Neuregelung in Absatz 2 kann die Auskunft nach näherer Maßgabe des Landesrechts auch im Wege des automatisierten Abrufs über das Internet erteilt werden. Dabei ist zu gewährleisten, dass dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten und an den Betroffenen übermittelten Daten gewährleisten. Der Nachweis der Urheberschaft des Antrags ist durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu führen. Die Vertraulichkeit der Daten ist durch die Verschlüsselung der Auskunft sicherzustellen. Zu den Anforderungen an Form und Inhalt des Antrags verweist § 8 Abs. 2 MRRG auf § 21 Abs. 1 a Satz 1 MRRG, der die Zulässigkeit der einfachen Melderegisterauskunft mittels elektronischen Verfahrens regelt.

Mit der Neuregelung in § 11 Abs. 2 MRRG wird die Abmeldepflicht bei Umzügen im Inland abgeschafft. Abgeschafft wurde auch die bisher in § 11 Abs. 3 MRRG normierte „Nebenmeldepflicht“ des Wohnungsgebers.

§ 11 Abs. 6 MRRG gibt den Ländern die Möglichkeit, die elektronische Anmeldung zuzulassen. Durch einen Verweis auf § 8 Abs. 2 Satz 2 MRRG werden die Meldebehörden zu den dem jeweiligen Stand der Technik entsprechenden Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit verpflichtet.

§ 21 Abs. 1 a MRRG regelt die Zulässigkeit der Erteilung einer einfachen Melderegisterauskunft auf automatisiert verarbeitbaren Datenträgern, durch Datenübertragung oder im Wege des auto-

matisierten Abrufs über das Internet. Einem automatisierten Abruf über das Internet kann der Betroffene widersprechen.

§ 21 Abs. 5 MRRG regelt die Auskunftssperre in den Fällen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange. Die Neufassung dieser Vorschrift hält zwar hinsichtlich der Voraussetzungen für die Eintragung einer Auskunftssperre im Melderegister an der bisherigen Rechtslage fest. Anders als nach der bisherigen Regelung des § 21 Abs. 5 MRRG ist jedoch nunmehr eine Risikoabwägung vorzunehmen, d.h., eine im Hinblick auf eine konkrete Gefährdungslage bewilligte Auskunftssperre greift danach nicht mehr, wenn nach Anhörung des Betroffenen ausgeschlossen werden kann, dass das der Meldebehörde vorliegende Auskunftsersuchen in einem denkbaren Zusammenhang mit den Gründen der Auskunftssperre steht.

In § 22 Abs. 1 MRRG, der die Melderegisterauskünfte an politische Parteien zur Wahlwerbezwecken regelt, werden die Meldebehörden verpflichtet, die Wahlberechtigten bei der Anmeldung und spätestens 8 Monate vor Wahlen durch öffentliche Bekanntmachung auf ihr Widerspruchsrecht hinzuweisen. Nach der bisherigen Regelung mussten die Wahlberechtigten nur bei der Anmeldung auf ihr Widerspruchsrecht hingewiesen werden.

Die Länder haben ihr Melderecht den geänderten und eingefügten Vorschriften des Melderechtsrahmengesetzes innerhalb von 2 Jahren nach dem Inkrafttreten dieses Gesetzes anzupassen. Bayern beabsichtigt in einem Gesetz zur Stärkung elektronischer Verwaltungstätigkeit Änderungen des Melderechtsrahmengesetzes in Landesrecht (Bayerisches Meldegesetz) umzusetzen.

Aus datenschutzrechtlicher Sicht ist zu begrüssen, dass der Bundesgesetzgeber von der zunächst bestehenden Absicht, eine gemeinsame Nutzung der Melderegister unterschiedlicher Meldebehörden zuzulassen, Abstand genommen hat. Verschiedene Forderungen der Datenschutzbeauftragten sind jedoch nicht berücksichtigt worden. So wurde die Hotelmeldepflicht nicht abgeschafft. Weiter wurde die einfache Melderegisterauskunft über das Internet nicht von der ausdrücklichen Einwilligung des Betroffenen abhängig gemacht. In diesen Fällen wurde jedoch zumindest ein Widerspruchsrecht geschaffen. Entgegen der Forderung der Datenschutzbeauftragten wurde die generelle Auskunftssperre in § 21 Abs. 5 MRRG zugunsten einer Risikoabwägung im Einzelfall aufgeweicht. Schließlich dürfen auch künftig Melderegisterauskünfte an politische Parteien zur Wahlwerbezwecken erteilt werden, sofern die Wahlberechtigten dieser Auskunfts-

erteilung nicht widersprochen haben. Da die Widerspruchslösung in weiten Kreisen der Bevölkerung unbekannt ist, haben die Datenschutzbeauftragten eine Einwilligungsregelung gefordert. Diese Forderung ist jedoch nicht berücksichtigt worden.

Die Entschließung der Datenschutzbeauftragten vom 08./09. März 2001 zur Novellierung des Melderechtsrahmengesetzes ist in der Anlage 3 abgedruckt.

10.2 Weitergabe von Melderegisterdaten an politische Parteien und an Adressbuchverlage

Ich erhalte regelmäßig Beschwerden von Bürgern, die mit der Weitergabe ihrer Melderegisterdaten an politische Parteien und mit der Veröffentlichung der Daten in Adressbüchern nicht einverstanden sind. Ich weise deshalb darauf hin, dass Bürger, die eine Weitergabe ihrer Daten an politische Parteien und an Adressbuchverlage nicht wollen, der Weitergabe widersprechen können. Sie müssen sich dazu an ihre Meldebehörde wenden.

Nach Art. 35 Abs. 1 Meldegesetz darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen und mit Abstimmungen in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familienname, Doktorgrad und Anschriften von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist, es sei denn, der Bürger hat dieser Weitergabe seiner Daten widersprochen. Ebenso kann der Betroffene nach Art. 35 Abs. 3 Meldegesetz der Weitergabe dieser Daten an Adressbuchverlage widersprechen. Nach dieser Vorschrift darf die Meldebehörde die o.g. Daten sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben und der Datenweitergabe nicht widersprochen haben, an Adressbuchverlage übermitteln.

10.3 Nutzung von Melderegisterdaten für Wahlwerbezwecke

Im Zusammenhang mit den Kommunalwahlen 2002 musste ich neben der Beantwortung einer Vielzahl von Anfragen von Bürgern und Kommunen auch Verstöße gegen datenschutzrechtliche Bestimmungen beanstanden.

In einem Fall hatte sich der zweite Bürgermeister einer Gemeinde während des Urlaubs des ersten Bürgermeisters ein Straßenverzeichnis mit den Anschriften, dem Wohnungsstatus und den Geburtsdaten aller Einwohner aus dem Melderegister beschafft und die Daten in seiner Eigenschaft als Bürgermeisterkandidat für Wahlwerbezwecke verwendet. Die Meldedaten wurden somit vom zweiten Bürgermeister nicht im Rahmen seiner dienstlichen Aufgabenerfüllung als Vertreter des ersten Bürgermeisters verwendet. Für Wahlwerbezwecke wäre eine Übermittlung personenbezogener Daten nach Art. 35 Abs. 1 MeldeG möglich gewesen. Danach hätte die Partei, für die der zweite Bürgermeister kandidiert hat, einen Antrag auf Erteilung einer Melderegisterauskunft nach Art. 35 Abs. 1 MeldeG stellen müssen. Diese hätte dann in den sechs der Stimmabgaben vorangehenden Monaten Auskünfte aus dem Melderegister im Rahmen dieser Vorschrift erhalten können. Die Geburtsdaten der Betroffenen sowie der Status der Wohnungen hätten dabei nicht übermittelt werden dürfen; darüber hinaus hätten keinerlei Auskünfte erteilt werden dürfen über die Personen, die nicht wahlberechtigt sind sowie über Personen, die einer Datenweitergabe zu Wahlwerbezwecken widersprochen haben.

In einem anderen Falle musste ich eine Kommune beanstanden, deren erster Bürgermeister Daten aus dem Melderegister einschließlich der Geburtsdaten, die er zu seiner dienstlichen Aufgabenerfüllung erhalten hatte, an seinen Schwiegersohn, der für das Amt des ersten Bürgermeisters kandidierte, zu Wahlwerbezwecken weitergegeben hatte. Auch hier hätte die Partei, für die der Schwiegersohn des ersten Bürgermeister kandidierte, einen Antrag auf Erteilung einer Melderegisterauskunft nach Art. 35 Abs. 1 MeldeG stellen müssen. Bei einer zulässigen Auskunft im Rahmen dieser Vorschrift wären die Geburtsdaten nicht mitgeteilt worden.

Ich nehme diese Vorgänge zum Anlass darauf hinzuweisen, dass Kommunen politischen Parteien und Wählergruppen nur im Rahmen einer Melderegisterauskunft nach Art. 35 Abs. 1 MeldeG personenbezogene Daten ihrer Bürger für Wahlwerbezwecke übermitteln dürfen.

10.4 Regelmäßige Übermittlung von Melderegisterdaten an die Gebühreneinzugszentrale (GEZ)

Ich erhalte immer wieder Anfragen von Bürgern, die anlässlich eines Umzugs Post von der GEZ erhalten und wissen wollen, wie die GEZ davon Kenntnis erhalten konnte. Auch von der Presse, an die sich in diesem Zusammenhang Betroffene gewandt haben, bin ich dazu befragt worden.

Ich nehme diese Anfragen zum Anlass darauf hinzuweisen, dass die Meldebehörden nach Art. 31 Abs. 4 des Bayerischen Meldegesetzes in Verbindung mit § 12 a Abs. 1 der Bayerischen Meldedaten-Übermittlungsverordnung dem Bayerischen Rundfunk oder der von ihm nach dem Rundfunkgebührenstaatsvertrag beauftragten Stelle ist (= GEZ) zum Zweck der Erhebung und des Einzugs der Rundfunkgebühren im Fall der An- bzw. Abmeldung oder des Todes u.a. die Anschrift der volljährigen Einwohner übermitteln dürfen. Da diese Vorschrift offenbar weitgehend unbekannt ist rege ich an, dass die Kommunen gelegentlich in geeigneter Weise darauf hinweisen.

10.5 Online-Zugriff auf Meldedaten durch gemeindliche Unternehmen

Dem Amt für Abfallwirtschaft und Stadtreinigung einer Gemeinde wurde zur Ermittlung aktueller Adressen die Möglichkeit eines Online-Abrufs gem. Art. 31 Abs. 7 MeldeG aus dem Einwohnermelderegister eingeräumt, soweit dies für die Gebührenabrechnung erforderlich war. Als die Dienststelle in der Betriebsform eines Eigenbetriebs fortgeführt wurde, stellte sich die Frage, ob der Abfallwirtschafts- und Stadtreinigungsbetrieb nach wie vor als eine Einrichtung innerhalb der Gemeindeverwaltung im Sinn von Art. 31 Abs. 7 MeldeG angesehen werden kann. Zu der Frage, mit der sich die Gemeinde an mich gewandt hat, habe ich eine fachliche Stellungnahme des Staatsministeriums des Innern eingeholt.

Das Innenministerium vertritt darin die Auffassung, dass für die Auslegung des melderechtlichen Begriffs „innerhalb einer Gemeinde“ i.S.d. Art. 31 Abs. 7 Satz 1 MeldeG nicht auf die allein im Zusammenhang mit dem Betrieb des gemeindlichen Unternehmens zu sehende organisatorische und wirtschaftliche weitgehende Selbstständigkeit des Eigenbetriebs i.S.d. Art. 86 Nr. 1, Art. 88 Abs. 1 Bayerische Gemeindeordnung (GO) abzustellen sei; entscheidend sei vielmehr die rechtliche Unselbstständigkeit des Eigenbetriebes. Der Eigenbetrieb sei als eine weitere Behörde der Gemeinde zu verstehen (vgl. hierzu auch Niese in Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 2 Rn. 22). Die Weitergabe von Daten vom Meldeamt an den gemeindlichen Eigenbetrieb stelle sich daher als Datenübermittlung zwischen zwei Behörden der Gemeinde dar, die jedoch **innerhalb der Gemeinde** erfolge.

Soweit ein Eigenbetrieb nicht am öffentlichen Wettbewerb teilnehme, richte sich die Datenübermittlung somit nach Art. 31 Abs. 7 MeldeG. Eine Differenzierung sei dann vorzunehmen,

wenn der Eigenbetrieb am allgemeinen Markt Leistungen anbiete, die auch andere anbieten, und ihm keine (rechtliche oder faktische) Monopolstellung zukomme, insbesondere kein Anschluss- und Benutzungszwang bestehe. Eine Datenübermittlung an den Eigenbetrieb werde in diesen Fällen der an private Stellen gleichgestellt, die nur unter den Voraussetzungen des Art. 34 MeldeG zulässig sei.

Die o. g. Auffassung des Bayerischen Staatsministeriums des Innern teile ich. Aus datenschutzrechtlicher Sicht halte ich eine Datenübermittlung an einen Eigenbetrieb, der **nicht** am öffentlichen Wettbewerb teilnimmt, datenschutzrechtlich nach Art. 31 Abs. 7 Satz 1 MeldeG somit für zulässig. Da regelmäßige Datenübermittlungen innerhalb der Gemeinde keiner besonderen Rechtsgrundlage nach Art. 31 Abs. 4 MeldeG bedürfen, halte ich auch regelmäßige automatische Datenübermittlungen von der Meldebehörde an diesen Eigenbetrieb für zulässig. Bei Eigenbetrieben, die am Wettbewerb teilnehmen, ist Art. 31 Abs. 7 MeldeG jedoch **nicht** anwendbar. Dies gilt auch für selbstständige Kommunalunternehmen des öffentlichen Rechts (Art. 89 GO i.V.m. Verordnung über Kommunalunternehmen - KUV - vom 19.03.1998) sowie für gemeindliche Unternehmen in Privatrechtsform (GmbH, AG).

Da im vorliegenden Fall der o. g. Eigenbetrieb der Gemeinde (auch) abfallwirtschaftliche Aufgaben wahrnimmt, ist zumindest für den Abfallentsorgungsbereich, sofern ein Anschluss- und Benutzungszwang besteht, die Online-Übermittlung von Meldedaten an den Eigenbetrieb auf der Grundlage des Art. 31 Abs. 7 Satz 1 MeldeG datenschutzrechtlich zulässig.

10.6 Datenschutz bei erweiterten Melderegisterauskünften, insbesondere im vereinfachten Verfahren nach Ziffer 34.3.2 VollzBekMeldeG

Eine Meldebehörde hat mir mitgeteilt, dass einige der in Bayern tätigen Auskunfteien im Wege der sog. „erweiterten Melderegisterauskunft im vereinfachten Verfahren“ gemäß Ziffer 34.3.2 der Vollzugsbekanntmachung zum Meldegesetz Daten abzufragen versuchen, die ihnen nicht zustehen. Ich habe das Bayerische Staatsministerium des Innern als zuständige oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich davon in Kenntnis gesetzt.

Das Bayerische Staatsministerium des Innern bestätigte, dass die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich bei ihren regelmäßigen Überprüfungen von Auskunfteien festgestellt haben, dass einige Auskunfteien Anfrageformblätter mit Fragen gegenüber den Meldebehörden verwendet haben, die die Meldebehörden gegenüber Privaten nicht beantworten dürfen („verheiratet mit wem?“) oder nur nach Glaubhaftmachung eines berechtigten Interesses („verheiratet?“). Die Aufsichtsbehörden haben gegenüber den Auskunfteien auf die künftige Verwendung korrekter Antragsformulare hingewirkt.

Aufgrund der Missbrauchsfälle habe ich bei der Überprüfung einer Gemeinde vor Ort daher auch die Praxis der Auskunftserteilung durch die Meldebehörde bei Anfragen von Auskunfteien einbezogen. Dabei habe ich festgestellt, dass auch in dieser Gemeinde von einer Auskunftei teilweise unzulässige Daten aus dem Melderegister (insbesondere über den Familienstand, Angaben zum Ehepartner) begehrt wurden. Da Auskünfte aus dem Melderegister an private Stellen, insbesondere an Auskunfteien, einen beträchtlichen Anteil aller Melderegisterauskünfte durch die Meldebehörde ausmachen, möchte ich hier auf Folgendes hinweisen:

1. Anfrageformulare von Auskunfteien

   In gemeinsamen Gesprächen zwischen dem Bayerischen Staatsministerium des Innern und den Spitzenverbänden der Auskunfteien wurde bereits vor mehreren Jahren ein Verfahren erarbeitet, das standardmäßige erweiterte Melderegisterauskünfte in einem vereinfachten Verfahren zulässt. Das Ergebnis dieser Gespräche ist in Ziffer 34.3.2 der Vollzugsbekanntmachung zum Meldegesetz (VollzBekMeldeG) eingegangen. In den Anfrageformularen von Auskunfteien dürfen demnach nur die in Art. 34 Abs. 1 und Abs. 2 Bayerisches Meldegesetz (MeldeG) in Verbindung mit Ziffer 34.3.2 VollzBekMeldeG genannten Daten nachgefragt werden.

   In den meisten Fällen werden von den Auskunfteien nicht alle Daten der erweiterten Auskunft benötigt. Im Wege der vereinfachten Form dürfen daher nur Vor- und Familienname, früherer Familienname, Anschriften, frühere Anschriften (nur wenn sie nicht länger als fünf Jahre zurückliegen), Tag der Geburt, Tag des Ein- und Auszugs und Sterbetag übermittelt werden (Ziffer 34.3.2 VollzBekMeldeG). Hierbei ist es ausreichend, wenn das berechtigte Interesse an der Kenntnis der Daten unter genauer Bezeichnung schlüssig vor-

getragen wird. Weitere Daten der erweiterten Auskunft können nur mit jeweiliger Einzelbegründung mitgeteilt werden. Zur Glaubhaftmachung jedes einzelnen Datums sind geeignete Unterlagen beizubringen (z. B. Vertragsunterlagen). Die Daten ergeben sich aus Art. 34 Abs. 2 MeldeG (Ziffer 34.4 VollzBekMeldeG).

Die Meldebehörden sollten die von Auskunfteien verwendeten Formulare auch in Zukunft sorgfältig dahin gehend überprüfen, ob nur die in Art. 34 Abs. 1 und 2 MeldeG genannten Daten erfragt werden **und** ob die Anfrageformulare mit der Vollzugsbekanntmachung im Einklang stehen. Sollte dies nicht der Fall sein, so sollte die Regierung von Mittelfranken als die für Bayern zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich informiert werden.

2. Verfahren bei Vorliegen einer Auskunftssperre nach Art. 34 Abs. 5 MeldeG

Nach Art. 34 Abs. 5 MeldeG ist jede Melderegisterauskunft unzulässig, wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, dass ihm oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Die von der Meldebehörde nach Art. 34 Abs. 5 MeldeG eingerichtete Auskunftssperre wirkt für alle Arten der Datenübermittlungen an Private (einfache Melderegisterauskunft nach Art. 34 Abs. 1 MeldeG, erweiterte Melderegisterauskunft nach Art. 34 Abs. 2 MeldeG und Gruppenauskünfte nach Art. 34 Abs. 3 MeldeG sowie nach Art. 35 Abs. 1 bis 3 MeldeG). Auf Datenübermittlungen an Behörden und an öffentlich-rechtliche Religionsgesellschaften hat die Auskunftssperre keinen Einfluss.

Hat die Meldebehörde eine Auskunftssperre nach Art. 34 Abs. 5 MeldeG eingerichtet und häufen sich anschließend die Auskunftsersuchen, insbesondere von Gläubigern des betroffenen Einwohners, so ist zu vermuten, dass der Einwohner möglicherweise von seinem Schutzrecht missbräuchlich Gebrauch macht. Die Meldebehörde sollte den betroffenen Einwohner hierauf hinweisen und ggf. die Auskunftssperre aufheben (siehe auch Ziffer 34.8 VollzBekMeldeG). Sofern die Anhörung des Betroffenen ergibt, dass eine Gefährdung zwar nach wie vor besteht, aber Auskünfte an Gläubiger diese Gefährdung nicht

beeinträchtigen, kann diese Art von Auskunftsersuchen einvernehmlich mit dem betroffenen Einwohner von der Auskunftssperre ausgenommen werden.

3. Unterrichtung des Betroffenen bei Erteilung einer erweiterten Melderegisterauskunft

Nach Auskunft der überprüften Gemeinde herrscht bei den Meldebehörden oft Unklarheit hinsichtlich der Frage, wann die Voraussetzungen für die Unterrichtung des Betroffenen bei einer erweiterten Melderegisterauskunft gegeben sind. Nach Art. 34 Abs. 2 Satz 2 MeldeG hat die Meldebehörde den Betroffenen über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten. Dies gilt nicht, wenn der Datenempfänger ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, glaubhaft gemacht hat. Gemäß Ziffer 34.5 VollzBekMeldeG ist das rechtliche Interesse stärker als das berechtigte Interesse. Der Meldebehörde muss das rechtliche Interesse dargelegt werden (z. B. Vollstreckungstitel o. ä.). Bonitätsprüfungen vor Eingehen eines Rechtsverhältnisses stellen keine rechtlichen, wohl aber in der Regel berechtigte Interessen dar (Ziffer 34.5 VollzBekMeldeG).

Durch die Benachrichtigung soll der betroffene Einwohner die Möglichkeit erhalten, die Richtigkeit der über ihn erteilten Auskunft zu kontrollieren. Gleichzeitig soll eine im allgemeinen und speziellen Datenschutzinteresse liegende Transparenz der Datenverarbeitung durch die Meldebehörde erreicht werden. Das rechtliche Interesse ist ein Teilbereich des berechtigten Interesses. Ein rechtliches Interesse ist anzunehmen, wenn bestehende Unsicherheiten über ein Rechtsverhältnis zu klären sind oder Rechtsansprüche durchgesetzt werden sollen. Bloße vorvertragliche Beziehungen, vor allem auch das Bedürfnis einer Bonitätsprüfung, z. B. Prüfung der evtl. Zahlungsunfähigkeit vor Eingehung eines geschäftlichen Risikos, sind zwar ein berechtigtes, aber kein rechtliches Interesse. Die Meldebehörde hat bei der Glaubhaftmachung des Interesses an der Melderegisterauskunft besonders darauf zu achten, dass auch tatsächlich ein rechtliches Interesse vorliegt. Nur dann ist sie von der Verpflichtung zur Unterrichtung des betroffenen Einwohners entbunden (siehe hierzu Kommentar von Böttcher zum Pass-, Ausweis- und Melderecht in Bayern, Art. 34, Rdnr. 14).

In Zweifelsfällen sollte die Meldebehörde konkret beim Auskunftsbegehrenden nachfra-

gen, ob die Anfrage tatsächlich auf einem rechtlichen Interesse beruht. Bei allen anderen Anfragegründen ist i.d.R. ein Verzicht auf die Benachrichtigung des Betroffenen nicht gerechtfertigt. Falls eine Unterrichtung erforderlich ist, soll dem Betroffenen gemäß Art. 34 Abs. 2 Satz 2 MeldeG der Datenempfänger und der Inhalt der Auskunft übermittelt werden.

4. Telefonische Auskunftserteilung

In der Praxis werden Melderegisterauskünfte auch telefonisch erteilt, sofern der Auskunftsbegehrende der Meldebehörde persönlich bekannt ist. Ist der Auskunftsbegehrende der Meldebehörde nicht persönlich bekannt, so ruft die Meldebehörde in der Regel den Anfragenden (ggf. über die Zentrale) zurück.

Das Meldegesetz sieht eine besondere Form der Auskunftserteilung aus dem Melderegister nicht vor. Die Auskunft kann schriftlich, mündlich und in eiligen Ausnahmefällen auch fernmündlich erteilt werden. Es wird empfohlen, telefonische Auskünfte **nur** in eiligen Ausnahmefällen zu erteilen, da bei telefonischen Anfragen Manipulationsversuche nicht ausgeschlossen werden können. Auch Hörfehler, die zu Personenverwechslungen oder unrichtigen Datenübermittlungen führen können, sind nicht auszuschließen. Der zuständige Sachbearbeiter sollte die Auskunftserteilung kurz schriftlich vermerken, damit ggf. eine Benachrichtigung des Betroffenen möglich ist. Erweiterte Melderegisterauskünfte sollten grundsätzlich nur schriftlich erteilt werden. Auf Ziffer 8.5 des 10. Tätigkeitsberichtes 1988 und Ziffer 8.3 des 14. Tätigkeitsberichtes 1992 wird hingewiesen.

11 Umweltfragen

11.1 Veröffentlichung der Standortdaten von Mobilfunksendeanlagen im Internet

Einige kreisfreie Gemeinden veröffentlichen im Internet Informationen über Mobilfunksendeanlagen. Genannt werden Straße und Hausnummer der Standorte sowie die Betreiber. Bei diesen

handelt es sich nicht um Einzelpersonen, sondern um Kapitalgesellschaften. Namen der betroffenen Grundstückseigentümer werden nicht veröffentlicht. Aus datenschutzrechtlicher Sicht vertrete ich zu der Frage, mit der ich auf Grund mehrerer Anfragen befasst war, folgende Auffassung:

Straßenbezeichnungen und Hausnummern der Standorte der Sendeanlagen können den jeweiligen Grundstückseigentümern über das Grundbuch zugeordnet werden. Soweit es sich bei den Grundstückseigentümern um natürliche Personen handelt, liegen personenbezogene Daten vor.

Die Mobilfunkbetreiber sind nach § 7 Abs. 1 der 26. Bundesimmissionsschutzverordnung verpflichtet, den Standort der Sendeanlage der zuständigen Behörde (Kreisverwaltungsbehörde) anzuzeigen. Für diese sind die Standortdaten umweltrelevante Daten im Sinn des Umweltinformationsgesetzes (UIG), zu denen grundsätzlich jedermann einen freien Zugang hat (§ 4 Abs. 1 UIG), soweit dieser Anspruch nicht nach § 7 oder § 8 UIG zu beschränken bzw. zu versagen ist. Soweit es sich um sichtbare Sendeanlagen handelt, sind Straßenbezeichnung und Hausnummer der Sendeanlagen offenkundige Daten und einer Veröffentlichung dieser Daten entgegenstehende Belange betroffener Dritter nicht ersichtlich. Einer Einstellung dieser Daten in das Internet habe ich deshalb nicht widersprochen. Ich weise aber darauf hin, dass eine ausdrückliche Regelung über eine solche Veröffentlichung im Bundesimmissionsschutzgesetz fehlt. Die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung auf diese Lücke hingewiesen und eine klare gesetzliche Regelung gefordert (Anlage Nr. 24).

Bei verdeckten Sendeanlagen, die somit nicht offenkundig sind, ist eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung des betroffenen Grundstückseigentümers und dem Interesse der Allgemeinheit an einem freien Zugang zu Umweltinformationen vorzunehmen. Dazu müssen die Betroffenen gemäß § 8 Abs. 2 UIG angehört werden. Von einem generell überwiegenden, einer Veröffentlichung der Informationen entgegenstehenden schutzwürdigen Interesse der betroffenen Grundstückseigentümer kann dabei im Rahmen der Abwägung grundsätzlich nicht ausgegangen werden, zumal diese die von ihrem Grundstück ausgehende Umweltrelevanz bewusst in Kauf nehmen und vom Betrieb der Anlage wirtschaftlich profitieren.

Gegen die Veröffentlichung der Namen der betroffenen Grundstückseigentümer bestünden datenschutzrechtliche Bedenken. Hier würden die schutzwürdigen Interessen der betroffenen

Grundstückseigentümer an der Geheimhaltung ihrer Daten das berechtigte Informationsinteresse der Allgemeinheit überwiegen.

12 Steuerverwaltung

12.1 Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung

Bereits in der Vergangenheit habe ich mehrfach von Bemühungen der Datenschutzbeauftragten des Bundes und der Länder berichtet, die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung zu erreichen (vgl. 16. Tätigkeitsbericht Nr. 11.1, 17. Tätigkeitsbericht Nr. 11.1). Diese Bemühungen sind bisher am Widerstand der Finanzverwaltung gescheitert. Nun ist wieder Bewegung in die Sache gekommen und es sind Fortschritte erkennbar.
Der Bundesbeauftragte für den Datenschutz hat zur inzwischen gewünschten Beratung des Bundesministers der Finanzen eine Bund/Länderarbeitsgruppe einberufen, an der auch ich mich beteiligt habe. Im Ergebnis wurden in der Arbeitsgruppe detaillierte Vorschläge für datenschutzrechtlich erforderliche bzw. wünschenswerte Änderungen und Ergänzungen der Abgabenordnung erarbeitet.

Als wesentliche Punkte sind insbesondere zu nennen:

- Regelung des Akteneinsichts- bzw. Auskunftsrechts
- Regelung der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (Outsourcing)
- Regelung von Aufbewahrungsfristen, Löschung und Sperrung von Daten.

Ich gehe davon aus, dass auf Seiten der Finanzverwaltung nunmehr kein Hinderungsgrund mehr für den Eintritt in eine allfällige Diskussion besteht und das erwähnte Papier eine gute Diskussionsgrundlage darstellt.

12.2 Elektronische Lohnsteuerkarte (ElsterLohn)

Zum Projekt der Elektronischen Lohnsteuerkarte finden sich grundsätzliche Ausführungen bereits in meinem 19. Tätigkeitsbericht unter Nr. 11.3. Meine dort geäußerte Auffassung gilt unverändert fort.

Das Staatsministerium der Finanzen betreibt das Projekt mit Hochdruck und beabsichtigt in kürze eine Pilotierung. Aufgrund der mir zu Verfügung gestellten aktuellen Projektunterlagen habe ich aus datenschutzrechtlicher Sicht erneut Stellung genommen.

Ich habe insbesondere darauf hingewiesen, dass durch das vorgesehene Verfahren vom Grundsatz der Datenerhebung beim Betroffenen (hier: Arbeitnehmer) abgewichen wird. Ein derartiger Eingriff in das informationelle Selbstbestimmungsrecht ist nach den Ausführungen des Bundesverfassungsgerichts zum Volkszählungsgesetz (BVerfGE 65, 1/44) nur im überwiegenden Allgemeininteresse, also nicht nur einseitig auf die Interessen einzelner Verfahrensbeteiligter (hier: Finanzverwaltung und Arbeitgeber) beschränkt, und nur aufgrund eines normenklaren Gesetzes zulässig.

Ich habe die Auffassung vertreten, dass auch bereits für die Pilotierungsphase die entsprechenden gesetzlichen Vorschriften vorliegen müssen. Sollte dies nicht der Fall sein, so ist nicht nur für Arbeitgeber sondern auch für jeden einzelnen Arbeitnehmer nur eine freiwillige Teilnahme an dem Pilotversuch denkbar. Art. 15 Abs. 1 BayDSG lässt einer anderen Interpretation keinen Raum. Es muss sichergestellt sein, dass die Einwilligung der Arbeitnehmer ohne Zwang durch den Arbeitgeber erfolgt.

Ausweislich der mir übermittelten Projektunterlagen soll die für den elektronischen Datenaustausch vorgesehene Identifikationsnummer (eTin) beim flächendeckenden Einsatz des Verfahrens, im Gegensatz zum Pilotverfahren, nicht beim Arbeitgeber, sondern bei den die Lohnsteuerkarten ausstellenden kommunalen Meldebehörden ermittelt und gespeichert werden. Ich musste das Staatsministerium darauf hinweisen, dass eine derartige Speicherung der eTin im Melderegister eine Ergänzung von Art. 3 des Bayer. Meldegesetzes zwingend erforderlich macht.

Die aktuellen Projektunterlagen gehen davon aus, dass die von den Arbeitgebern elektronisch übermittelten Lohnsteuerdaten zentral für das jeweilige Bundesland gespeichert werden und für die Finanzbehörden die Möglichkeit einer bundesweiten Auswertung vorgesehen wird. Ich habe darauf hingewiesen, dass derartige Zentraldateien und insbesondere der automatisierte Zugriff darauf erhebliche datenschutzrechtliche Fragen aufwerfen. Die mir noch nicht bekannten Einzelheiten des geplanten Zugriffsverfahrens werden kritisch zu würdigen sein. Ich halte in diesem Zusammenhang die Einbeziehung des Abrufverfahrens in die geplante Steuerdatenabruf-Verordnung für erforderlich.

12.3 Neuregelung des Steuerabzugs bei Bauleistungen und Erweiterung der Angaben auf Rechnungen

Der Gesetzgeber hat im Rahmen des Gesetzes zur Eindämmung illegaler Betätigung im Baugewerbe vom 30.08.2001 u.a. ein Steuerabzugsverfahren bei Bauleistungen eingeführt. Weiterhin wurde durch das Steuerverkürzungsbekämpfungsgesetz vom 19.12.2001 u.a. der Umfang der auf einer Rechnung aufzuführenden Angaben erweitert. Beide Neuregelungen waren Ausgangspunkt mehrerer Eingaben, wobei die mit den genannten Bestimmungen verbundene Streuung von persönlichen Angaben und steuerlichen Merkmalen im Vordergrund stand.

Hauptinhalt der Neuregelung des Steuerabzugs bei Bauleistungen ist die grundsätzliche Verpflichtung des Leistungsempfängers, von der Gegenleistung an den Erbringer der Bauleistung einen Steuerabzug von 15 v.H. vorzunehmen und an die Steuerverwaltung abzuführen (vgl. § 48 ff. EStG). Der Leistungsempfänger haftet ausdrücklich für einen nicht oder zu niedrig abgeführten Abzugsbetrag.

Der Leistende kann den Steuerabzug allerdings vermeiden, indem er dem Leistungsempfänger eine vom Finanzamt ausgestellte Freistellungsbescheinigung vorlegt. Der Inhalt der Freistellungsbescheinigung wird durch § 48 b Abs. 3 EStG geregelt. Neben den dort aufgeführten Angaben beinhalteten mir vorgelegte Bescheinigungen bei Einzelunternehmern auch das Geburtsdatum des Firmeninhabers, was ich nicht für erforderlich halte. Ich habe mich in diesem Zusammenhang an das Staatsministerium der Finanzen gewandt. Das Staatsministerium hat eine Abstimmung auf Bund-Länder-Ebene mit dem Ergebnis eingeleitet, dass dieses Merkmal zukünftig entfallen wird.

In den Eingaben zur sog. Bauleistungssteuer wurde auch angesprochen, dass durch Vorlage der Freistellungsbescheinigung Dritte Kenntnis von der Steuernummer des Bauleisters erlangten. Eine weitere und wohl wesentlich umfangreichere Kenntnisnahme der Steuernummer von Unternehmern/Unternehmen durch Dritte ist durch die ab 01.07.2002 in Kraft getretene Ergänzung des § 14 UStG durch das bereits erwähnte Steuerverkürzungsbekämpfungsgesetz zu erwarten. Danach ist ein Unternehmer bei der Ausführung von Lieferungen und sonstigen Leistungen an einen anderen Unternehmer auf dessen Verlangen verpflichtet, eine Rechnung auszustellen, in der - und das ist neu - auch die Steuernummer anzugeben ist. Die Eingabeführer befürchten, dass mit Kenntnis der Steuernummer Dritte, gerade bei telefonischer Auskunftserteilung , von den Finanzämtern unzulässigerweise durch das Steuergeheimnis geschützte Daten erlangen könnten. Ich habe das Staatsministerium auf diese Problematik hingewiesen. Das Staatsministerium hat inzwischen die Finanzämter über die Problematik informiert und Verhaltensregelungen erstellt.

12.4 Auswertung von Lohnsteuerkarten auf Schwerbehinderteneigenschaft

In meinem 12. Tätigkeitsbericht habe ich unter Nr. 10.3 zur Frage der Offenbarung der Schwerbehinderteneigenschaft gegenüber dem Dienstherrn Stellung genommen. Im Ergebnis war festzuhalten, dass durchaus Fallkonstellationen denkbar sind, in denen der Arbeitnehmer nicht verpflichtet ist, seinem Arbeitgeber eine bestehende Schwerbehinderung zu offenbaren. In diesem Zusammenhang wurde ich von einer Kommune gefragt, ob es zulässig sei, die Lohnsteuerkarten auf Einträge eines steuerlichen Freibetrags wegen Körperbehinderung nach § 33 b EStG auszuwerten und mit der beim Arbeitgeber vorhandenen Schwerbehindertendatei abzugleichen.

Ich habe der Kommune mitgeteilt, dass nach § 39 b Abs. 1 Satz 4 EStG die auf der Lohnsteuerkarte eingetragenen Merkmale nur für Zwecke der Einbehaltung der Lohnsteuer verwertet werden dürfen. Die gesetzlich normierte Zweckbestimmung stand damit der beabsichtigten Auswertung entgegen. Ich habe dabei nicht verkannt, dass die Nichtangabe einer bestehenden Schwerbehinderung beim Arbeitgeber die Pflicht zur Abführung einer Ausgleichsabgabe nach § 77 SGB IX auslösen kann. Ich gehe aber davon aus, dass die zu entrichtende Abgabe durch den in diesem Fall eintretenden Verzicht auf Sonderurlaub gem. § 125 SGB IX mehr als ausgeglichen wird.

12.5 Eintragung eines Pauschbetrags für Behinderte auf der Lohnsteuerkarte

Die Steuervergünstigung wegen Körperbehinderung kann durch die Eintragung eines Freibetrags im Rahmen eines Antrags auf Lohnsteuerermäßigungen oder auch durch Geltendmachung im Rahmen der Einkommensteuerveranlagung in Anspruch genommen werden.

Wird ein Antrag auf Lohnsteuerermäßigung gestellt, hat dies in der Regel die Gewährung der Vergünstigung während der Geltungsdauer des Behindertenausweises zur Folge. Die Finanzämter weisen in diesen Fällen die Gemeinden in den Folgejahren an, den Freibetrag bereits bei Ausstellung der Lohnsteuerkarte zu berücksichtigen. Mit dem praktizierten Verfahren soll eine sich jährlich wiederholende Neubeantragung vermieden werden, was sicherlich im Interesse vieler Betroffener liegt.

In meinem 16. Tätigkeitsbericht habe ich unter Nr. 11.4 dargelegt, dass auch Fälle denkbar sind, in denen der Steuerpflichtige künftigen Datenübermittlungen an die Gemeinde widersprechen und die Eintragung des Freibetrags auf der Lohnsteuerkarte durch das Finanzamt selbst oder im Rahmen der Einkommensteuerveranlagung erreichen will. Das Staatsministerium der Finanzen hat meinen Vorstoß auf Grund eines befürchteten Verwaltungsmehraufwands bei den Finanzämtern abgelehnt.

Probleme können sich aktuell im Zusammenhang mit der Berechnung der Nettobezüge bei Gewährung von Altersteilzeit nach Art. 80 d BayBG ergeben. Bei Berechnung dieser Nettobezüge werden die auf der Lohnsteuerkarte eingetragenen Freibeträge ausnahmslos berücksichtigt. Dies führt letztlich zu einer Erhöhung der Nettodienstbezüge und zu einer Minderung des Altersteilzeitzuschlags, welche auch nach Durchführung der Steuerveranlagung nicht mehr ausgeglichen wird.

Dieses Ergebnis kann nur dadurch vermieden werden, dass der Steuerpflichtige sich keinen Freibetrag auf der Lohnsteuerkarte (mehr) eintragen lässt und die entsprechende steuerliche Vergünstigung erst im Rahmen des Veranlagungsverfahrens geltend macht.

Im Hinblick auf das eingangs erwähnte „automatische“ Eintragungsverfahren eines Freibetrags wegen Körperbehinderung muss deshalb für den Steuerpflichtigen die Möglichkeit bestehen, der

Eintragung für künftige Jahre zu widersprechen, um für ihn ungünstige Rechtsfolgen zu vermeiden.

Ich habe mich in diesem Sinne erneut an das Staatsministerium der Finanzen gewandt. Das Staatsministerium hat mir mitgeteilt, dass es zumindest in diesen Fällen einen Antrag auf Änderung des Freibetrags für Behinderte beim zuständigen Finanzamt für zulässig hält. Der Antrag des Steuerpflichtigen auf Änderung des von der Gemeinde von Amts wegen nach Anweisung des Finanzamts gem. § 39 a Abs. 2 Satz 1 EStG bei der Ausstellung der Lohnsteuerkarte eingetragenen Pauschbetrags für Behinderte zieht in diesen Fällen eine neue Anweisung des Finanzamts an die Gemeinde zur geänderten Berücksichtigung des Pauschbetrags in den Folgejahren nach sich.

12.6 Rücksendung von Belegen an Steuerpflichtige

Auf Grund mehrerer Eingaben wurde ich auf folgenden Sachverhalt aufmerksam:

Bei der Rücksendung von eingereichten Belegen an die Steuerpflichtigen wurden von Bediensteten verschiedener Finanzämter Belege (z.B. Beitragsrechnungen), die die Anschrift der Steuerpflichtigen enthielten, als Deckblatt benutzt. Wahrscheinlich sollte durch diese Sachbehandlung das Fertigen einer Kurzmitteilung oder eines ähnlichen finanzamtlichen Deckblatts eingespart werden. Diese Handlungsweise führte in den an mich herangetragenen Fällen deshalb zu Problemen, weil die Steuerpflichtigen inzwischen jeweils verzogen waren. Die Postbediensteten schickten die Briefe des Finanzamtes an die im Sichtfenster des Briefkuverts lesbaren Adressen der vermeintlichen Absender, in vorliegenden Fällen von Privatfirmen, deren Rechnungen die Steuerpflichtigen steuerlich geltend gemacht hatten. In den genannten Fällen kam es deshalb zu einer unzulässigen Durchbrechung des Steuergeheimnisses. Man konnte zwar einwenden, dass sich auf den Kuverts auch die Poststempel der absendenden Finanzämter befunden hatten. Festzuhalten blieb aber, dass die unzulässige Durchbrechung des Steuergeheimnisses bei der Verwendung entsprechender finanzamtlicher Deckblätter zuverlässig hätte vermieden werden können.

Die eingeschalteten Oberfinanzdirektionen München und Nürnberg haben diese Auffassung geteilt und die nachgeordneten Dienststellen entsprechend angewiesen. Darüber hinaus wurde mir

mitgeteilt, dass beabsichtigt sei, künftig die Vorausverfügung auf den Kuverts insoweit zu ändern, als im Falle einer Adressänderung - soweit bekannt - eine Anschriftenberichtigungskarte an die absendende Finanzbehörde übermittelt und die Sendung an die neue Adresse zugestellt werde.

12.7 Datenschutz bei der Zustellung durch Finanzbehörden

Auch in abgaberechtlichen Angelegenheiten erfolgt in bestimmten Fällen die Zustellung von Schriftstücken mittels Postzustellungsurkunde. Neben dem Geschäftszeichen der Behörde wird dabei auch der Betreff der Sache angegeben. In dem mir vorgelegten Sachverhalt lautete dieser „Verbot der unbef. Hilfeleistung in Steuers.“, was, mit nur wenig Fantasie, in der Langfassung „Verbot der unbefugten Hilfeleistung in Steuersachen“ bedeutet.

Auf Grund der Rechtsprechung des Bundesfinanzhofes sind die Finanzbehörden gehalten, bei der Zustellung mit Postzustellungsurkunde sicherzustellen, dass aus der auf der Urkunde und dem Briefumschlag anzugebenden Geschäftsnummer der Inhalt der zugestellten Sendung eindeutig zu entnehmen ist. Nach Ansicht des Gerichts reicht dazu die bloße Angabe der Steuernummer als Geschäftszeichen nicht aus. Die Geschäftsnummer muss vielmehr so gebildet werden, dass sie zweifelsfrei die Identifizierung des Inhalts der Sendung durch die Angabe auf dem Briefumschlag ermöglicht.

Auch unter Berücksichtigung dieser Rechtsprechung bin ich der Auffassung, dass weniger sprechende“ Zusätze ausreichen. Die Finanzbehörde hat mir neutrale Zusätze vorgeschlagen, die das Problem künftig wesentlich entschärfen werden. In vorliegendem Sachverhalt wurde bspw. an die Geschäftsnummer und das Datum das Wort Belehrung in abgekürzter Form angehängt.

13 Personalwesen

13.1 Verarbeitung und Nutzung von Personalaktendaten

13.1.1 Übermittlung von Personaldaten an Krankenkassen und an die Presse

Es erreichen mich immer wieder Anfragen von Behörden zur Zulässigkeit der Weitergabe der Adressen neu eingestellter Beamtenanwärter oder Auszubildender an (gesetzliche und private) Krankenkassen.

Nach meiner Auffassung sind die Vorschriften über das Personalaktenrecht der Beamten (Art. 100 ff. BayBG) analog auch auf die nichtverbeamteten Beschäftigten des öffentlichen Dienstes anzuwenden, da sie allgemein gültige Schutzprinzipien für Arbeitnehmer enthalten. Daher lässt sich diese Frage für beide Personengruppen anhand Art. 100 e Abs. 2 Satz 1 BayBG beantworten, wonach **Auskünfte an Dritte** nur mit **Einwilligung** des Beamten erteilt werden dürfen, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. Im Übrigen kommt man zum gleichen Ergebnis, wenn man ohne analoge Anwendung des Personalaktenrechts der Beamten die Vorschrift des Art. 19 Abs. 1 Nr. 2 BayDSG anwendet.

Die Krankenkassen sind Dritte im Sinne dieser Vorschrift, obige Ausnahmen liegen offensichtlich nicht vor. Daher dürfen ihnen Auskünfte nur mit Einwilligung des Betroffenen erteilt werden, wobei diesem gemäß Art. 100 e Abs. 2 Satz 2 BayBG Inhalt und Empfänger der Auskunft schriftlich mitzuteilen wären.

Obige Grundsätze müssen öffentliche Stellen auch in ihrer Pressearbeit beachten. Ein ehemaliger Bediensteter einer Kommune hatte sich an mich gewandt, weil sein damaliger Dienstherr in einem Leserbrief in der lokalen Tageszeitung Personalaktendaten offengelegt hat. Ich habe diesen Vorgang beanstandet.

13.1.2 Kalendarische Übersichten über Abwesenheiten

Im Zeitalter der Verwaltungsmodernisierung und der Einführung der Kosten- und Leistungsrechnung werden an immer mehr Dienststellen Abwesenheitskalender oder Jahresübersichten über **Abwesenheiten** in Papierform oder in elektronischer Form geführt. Dazu ist aus datenschutzrechtlicher Sicht Folgendes anzumerken:

Beurteilungsgrundlage für diese Übersichten sind die Vorschriften des Personalaktenrechts für Beamte (Art. 100 ff. BayBG), die - wie bereits in Nr. 13.1.1 erwähnt - analog auch auf Angestellte und Arbeiter des öffentlichen Dienstes anzuwenden sind. Auch hier käme man gemäß Art. 17 Abs. 1 BayDSG, der sowohl das Erforderlichkeitsprinzip als auch das Zweckbindungsprinzip enthält, zu den gleichen Ergebnissen. Unterlagen über Erholungsurlaub und Erkrankungen etc. sind den **Personalaktendaten** zuzurechnen (vgl. Art. 100 a Abs. 1 Satz 2, Abs. 2 Satz 2 BayBG). Nach Art. 100 a Abs. 1 Satz 3 BayBG dürfen Personalaktendaten nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein. Das Verbot der anderweitigen Verwendung betrifft den Dienstherrn bzw. die Behörden oder Dienststellen des Dienstherrn, denen die Personalaktendaten zugänglich gemacht werden dürfen.

Bei der Bekanntgabe personenbezogener Abwesenheitsdaten an Behördenangehörige liegt eine Datennutzung im Sinne des Art. 4 Abs. 7 BayDSG vor, da es sich um die Weitergabe von Daten innerhalb der speichernden Stelle (vgl. Art. 4 Abs. 9 BayDSG) handelt. Zwecke der Personalwirtschaft im Sinne des Art. 100 a Abs. 1 Satz 3 BayBG sind im Hinblick auf organisatorische Fragen gegeben. Im Regelfall dürfte jedoch im Rahmen der dienstlichen Erforderlichkeit die Kenntnis der Abwesenheits**zeiten** ausreichen; sowohl die Gründe für eine Abwesenheit als auch die nachträgliche Eintragung von Krankheitszeiten sind dagegen für diese Zwecke nicht erforderlich.

Soweit Datennutzungen über den dargestellten Umfang hinausgehen, wären sie nur mit der freiwilligen und informierten **Einwilligung** der Betroffenen (Art. 100 a Abs. 1 Satz 3 BayBG, Art. 15 Abs. 2 bis 4 BayDSG) zulässig. Für die Einholung einer solchen Einwilligung sehe ich jedoch keinen Grund. Die Aufstellungen sollten sich deswegen auf die Abwesenheitszeiten be-

schränken. Das gilt umsomehr, falls Dritten, z. B. Besuchern der Behörde, eine Einsichtnahme in die Übersichten möglich sein sollte (z. B. durch den „Standort“ des Kalenders), s. dazu Art. 100 e Abs. 2 Satz 1 BayBG.

13.1.3 Nutzung von Zeiterfassungsdaten

Anknüpfend an meine Ausführungen unter Nr. 13.1.2 gebe ich speziell zur Nutzung von Zeiterfassungsdaten beispielsweise durch Mitarbeiter und Mitarbeiterinnen im Rahmen eines mit der elektronischen Zeiterfassung gekoppelten Tableaus oder durch die zentrale Telefonvermittlung nachstehende Hinweise:

Auch **Zeiterfassungsunterlagen** (also Unterlagen über Erholungsurlaub, Erkrankungen, Dienstreisen, Dienstgänge etc.) sind **Personalaktendaten** und können in einem eigenen Teilakt bei der für diesen Aufgabenbereich zuständigen Stelle der Behörde geführt werden.

Unter Verweis auf Art. 100 a Abs. 1 Satz 3 BayBG ist auch hier im Hinblick auf organisatorische Fragen die Kenntnis von „anwesend“ und „abwesend“ und ggf. der Dauer der Abwesenheit in der Regel ausreichend. Abwesenheitsgründe sind nur bekannt zu geben, wenn dies im Einzelfall ausnahmsweise erforderlich ist.

Auch die entsprechende Information von Anrufenden durch die zentrale Telefonvermittlung (hier handelt es sich um Datenübermittlungen nach Art. 4 Abs. 6 Satz 2 Nr. 3 Buchstabe a BayDSG, weil Daten an Dritte (Art. 4 Abs. 10 BayDSG) weitergegeben werden) ist gemäß Art. 19 Abs. 1 Nr. 1, Art. 17 Abs. 1 Nr. 2 BayDSG nur in dem Umfang zulässig, wie sie für die Personalwirtschaft erforderlich ist. So halte ich die Verwendung von Urlaubs- und Krankheitsdaten ohne die freiwillige und informierte Einwilligung der Betroffenen gemäß Art. 100 a Abs. 1 Satz 3 und Art. 100 e Abs. 2 Satz 1 BayBG regelmäßig für nicht zulässig.

Damit scheidet eine institutionalisierte Unterrichtung der zentralen Telefonvermittlung, z. B. durch die generelle Weitergabe von Abwesenheitslisten, in denen auch die einzelnen Abwesenheitsgründe aufgeführt sind, aus.

Regelungen zur Nutzung der Zeiterfassungsdaten sind in einer **Dienstvereinbarung** (vgl. Art. 73 BayPVG) zur Arbeitszeiterfassung festzulegen.

13.1.4 Personaldaten im Intranet

In immer mehr Behörden gewinnt das **Intranet** an Bedeutung. Zur Veröffentlichung von Personaldaten von Mitarbeitern und Mitarbeiterinnen im Intranet gebe ich deshalb folgende Hinweise:

Nach dem m. A. auch auf den Tarifbereich analog anzuwendenden Art. 100 h Abs. 1 Satz 1 BayBG dürfen auch **Personalaktendaten in Dateien** nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet und genutzt werden. Zu den Personalaktendaten zählen die Daten der zum Personalakt gehörenden Unterlagen, d. h. aller Unterlagen (einschließlich der in Dateien gespeicherten), die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen, also der Personalverwaltung (Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses) dienen (vgl. Art. 100 a Abs. 1 Satz 2 BayBG). Daten, die z. B. im Zusammenhang mit Neueinstellungen, Arbeitsplatzwechsel, Dienstjubiläen, Verabschiedungen, Beförderungen und Höhergruppierungen veröffentlicht werden sollen, sind also den Personalaktendaten zuzuordnen.

Obwohl die Begriffe „Personalverwaltung und Personalwirtschaft“ in Art. 100 a Abs. 1 Satz 3 bzw. Art. 100 h Abs. 1 Satz 1 BayBG weit zu fassen sind, sind bei der Veröffentlichung von Mitarbeiterdaten im Intranet einer Behörde in der Regel diese Verwendungszwecke jedoch nicht gegeben. Ich halte deshalb die **Einwilligung** der Betroffenen grundsätzlich für erforderlich. Lediglich die Veröffentlichung offenkundiger Daten wie Familienname, Vorname, Amts- oder Dienstbezeichnung, Sachgebiet, Dienstzimmer, Nebenstellennummer, Funktionsübertragung ist im Intranet auch ohne Einwilligung zulässig, da derartige Angaben entsprechend einem unabweisbaren dienstlichen Bedürfnis behördenintern allgemein bekannt gemacht werden (durch Türschilder, Telefonverzeichnis, Geschäftsverteilungsplan). Diese Daten werden damit gemäß Art. 100 a Abs. 1 Satz 3, Art. 100 h Abs. 1 Satz 1 BayDSG in zulässiger Weise für Zwecke der Personalwirtschaft verwendet. Beim Organisationsreferat werden diese personenbezogenen Daten Teile der jeweiligen Sachakten, für die die Datenschutzvorschriften dieser Sachakten gelten, insbesondere Art. 17 ff. BayDSG. Die Zweckbestimmung dieser Daten bleibt auch als Sachaktendaten allein „Personalverwaltung und Personalwirtschaft“ (vgl. Kommentar zum BayDSG,

Wilde/Ehmann/Niese/Knoblauch, Handbuch XIV 3 e). Die Bekanntmachung der Daten (durch Türschilder, im Intranet) ist nach Art. 19 Abs. 1 Nr. 1, Art. 17 Abs. 1 Nr. 2 BayDSG zulässig, soweit dies für die Personalwirtschaft erforderlich ist. Eine Bekanntgabemöglichkeit besteht aber nur für die vorstehend genannten Daten. Soweit allerdings Personalmaßnahmen Rückschlüsse auf deren Grund und damit auf persönliche, private Verhältnisse der Bediensteten zulassen, wäre die Einwilligung der Betroffenen notwendig. Die Einholung einer solchen Einwilligung käme z. B. für Hausnachrichten unter der Rubrik „Namensänderung infolge Eheschließung“ in Betracht.

Im Übrigen verweise ich auch auf meine Orientierungshilfe „Veröffentlichung von Informationen im Internet und im Intranet“ (http://www.datenschutz-bayern.de/technik/orient/int-publ.htm).

13.1.5 Verwendung von Personalaktendaten in automatisierten Dateien

Im Zuge der Automatisierung werden verstärkt **Personalverwaltungsprogramme** in der öffentlichen Verwaltung eingesetzt. Dazu weise ich auf Folgendes hin:

Die Zulässigkeit der automatisierten Verarbeitung und Nutzung von **Personalaktendaten** richtet sich nach Art. 100 h Abs. 1 Satz 1 BayBG, wonach Personalaktendaten (Art. 100 a Abs. 1 Satz 2 BayBG) auch in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet und genutzt werden dürfen (s. dazu Art. 100 a Abs. 1 Satz 3 BayBG und meine Ausführungen unter Nr. 13.1.4). Durch automatisierte Dateien kann zwar die Verarbeitung und Nutzung der Personalaktendaten erleichtert und beschleunigt werden, der Verwendungszweck der Daten wird dadurch aber nicht erweitert. Durch technisch-organisatorische Maßnahmen muss gewährleistet werden, dass nur berechtigte Personen (vgl. Art. 100 a Abs. 3 BayBG) auf die Daten zugreifen können. Die Einwilligung des jeweiligen Beschäftigten ist für eine datenschutzrechtlich zulässige Verwendung von Personalaktendaten nicht erforderlich.

Art. 100 h Abs. 1 Satz 1 BayBG bestimmt den Verwendungszweck, trifft aber keine Aussage darüber, in welchem Umfang die Daten für die genannten Zwecke genutzt werden dürfen. Hier sind die allgemeinen datenschutzrechtlichen Grundsätze über die Notwendigkeit und Verhält-

nismäßigkeit der Verarbeitung personenbezogener Daten zu beachten. Zusätzliche Einschränkungen ergeben sich aus Art. 100 h Abs. 2 bis 4 BayBG.

Bei erstmaliger Speicherung ist dem Betroffenen die Art der über ihn gemäß Art. 100 h Abs. 1 BayBG gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist er zu benachrichtigen (Art. 100 h Abs. 5 Satz 1 BayBG). Ferner sind Dokumentationspflichten vorgesehen (Art. 100 h Abs. 5 Satz 2 BayBG).

Personalverwaltungsprogramme bedürfen gemäß Art. 26 Abs. 1 Satz 1 i.V.m. Abs. 3 Satz 2 BayDSG der **datenschutzrechtlichen Freigabe** durch den behördlichen Datenschutzbeauftragten. Art. 75 a Abs. 1 Nr. 2 BayPVG sieht eine Mitbestimmung des **Personalrats** bei der Einführung, Anwendung und erheblichen Änderung von automatisierten Verfahren zur Personalverwaltung vor.

13.2 Personalaktendaten in der Rechnungsprüfung

13.2.1 Zuleitung von Beschlussniederschriften des Personalausschusses an die Rechnungsprüfung

Eine Kommune hat die Frage an mich herangetragen, ob der **örtlichen Rechnungsprüfung alle** Entscheidungen des Personalausschusses zugeleitet werden dürfen.

Aus datenschutzrechtlicher Sicht ist hier grundsätzlich von einer zulässigen Zweckänderung gemäß Art. 17 Abs. 3 Satz 1 BayDSG („Rechnungsprüfung“) auszugehen. Es stellt sich jedoch die Frage, ob die Weiterleitung **aller Entscheidungen bzw. Beschlussniederschriften des Personalausschusses** an die Rechnungsprüfungsstelle zu deren Aufgabenerfüllung erforderlich ist (vgl. Art. 17 Abs. 1 Nr. 1 BayDSG).

Im Rahmen der Erforderlichkeit ist zu prüfen, ob eine Maßnahme objektiv geeignet und angemessen ist. Prinzipiell ist die Weiterleitung sämtlicher Beschlüsse zwar zur Aufgabenerfüllung der Rechnungsprüfung geeignet. Die Weiterleitung aller Beschlussniederschriften ist jedoch nicht angemessen. So dürfte die Weiterleitung von Tagesordnungen mit dem entsprechenden Betreff ausreichen. Anhand von Kurzprotokollen der Sitzungen des Personalausschusses können überdies geeignete Prüfungsgegenstände festgelegt werden. Zudem ist es auch möglich, stich-

probenartige Kontrollen vorzunehmen und sich hierzu die notwendigen Niederschriften vorlegen zu lassen. Dies sind im Vergleich zur Vorlage aller Beschlussniederschriften mildere Mittel.

Im Übrigen ist zu berücksichtigen, dass eine generelle Übermittlung zu einer parallelen Aktenführung bei der Rechnungsprüfung führt, die weitere Probleme (z. B. bei einer Löschung oder Vernichtung) mit sich bringen kann.

Ich halte deswegen eine pauschale Zuleitung der Personalausschussentscheidungen an die örtliche Rechnungsprüfung nicht für zulässig.

13.2.2 Einsicht in dienstliche Beurteilungen und Nutzung von Beihilfeunterlagen durch örtliche Rechnungsprüfer

Da ich vermehrt Anfragen zur Nutzung von **Personalaktendaten** (vgl. Art. 100 a Abs. 1 Satz 2, Abs. 2 Satz 1 BayBG) durch **örtliche Rechnungsprüfer** bekomme, gebe ich zur Einsichtnahme in dienstliche Beurteilungen und zur Nutzung von Beihilfeunterlagen in Abstimmung mit dem Bayer. Staatsministerium der Finanzen folgende Hinweise:

Interne Rechnungsprüfer einer Kommune haben ein Zugangsrecht zu Personalakten gemäß Art. 100 a Abs. 3 BayBG, dessen Schranken sich durch einen Ausgleich zwischen dem Schutz des Persönlichkeitsrechts der betroffenen Beamten und der Erhaltung und Förderung der Funktionsfähigkeit der Personalverwaltung, wozu auch die interne Kontrolle gehört, ergeben. Diese Vorschrift regelt den Zugang innerhalb der den Personalakt (Grundakt, Teilakten und Nebenakten) führenden Behörden. Die Einschränkung der Zugangsberechtigung gilt nicht nur für die Einsichtnahme in den (gesamten) Personalakt, sondern auch für die Zulässigkeit des Zugangs zu einzelnen zum Personalakt im materiellen Sinn gehörenden Vorgängen. Soweit die Personalaktendaten eine geeignete Grundlage oder Hilfe für die Entscheidungsfindung oder die sonstige Personalangelegenheit bilden, ist auch ihre Heranziehung nicht zu beanstanden.

Vor dem Hintergrund des Erforderlichkeitsprinzips halte ich die Einsichtnahme interner Rechnungsprüfer in **dienstliche Beurteilungen** von Bediensteten grundsätzlich nicht für zulässig.

Nr. 7.12 meines 14. Tätigkeitsberichts, in der ich zu dem Schluss kam, dass gegen eine stichprobenartige Überprüfung der Beihilfefestsetzungen durch die örtlichen Rechnungsprüfer keine Bedenken bestehen, ist im Hinblick auf die durch § 1 Nr. 22 des Zwölften Gesetzes zur Änderung beamtenrechtlicher Vorschriften vom 23.07.1994 (GVBl S. 611) in das Bayer. Beamtengesetz eingefügten Vorschriften (Art. 100 ff.) zu konkretisieren. Beihilfeakten werden wegen ihres hochsensiblen Inhalts besonders behandelt (vgl. Art. 100 b, Art. 100 g Abs. 2 BayBG). Bei der Nutzung von Beihilfeunterlagen durch örtliche Rechnungsprüfer ist zwischen **Beihilfeunterlagen**, die die Art der Erkrankung erkennen lassen, und den übrigen Beihilfeunterlagen zu differenzieren:

Beihilfeunterlagen, die die Art der Erkrankung erkennen lassen, nehmen wegen der besonderen Sensibilität der Daten eine Sonderstellung ein; diese wird durch die Schutzvorschrift des Art. 100 g Abs. 2 Satz 2 BayBG unterstrichen. Solche Daten dürfen auch von der für die Beihilfefestsetzung zuständigen Stelle nur solange als erforderlich verwendet und nicht an andere Stellen weitergegeben werden. Diese Sonderstellung verbietet eine Weitergabe dieser Unterlagen an kommunale Rechnungsprüfer, soweit nicht eine Einwilligung des betroffenen Beamten vorliegt, wobei ich nicht sehe, in welchen Fällen derartige Unterlagen für die Tätigkeit der Rechnungsprüfer von Bedeutung sein sollen.

Die Weitergabe der übrigen Beihilfeunterlagen richtet sich nach Art. 100 b Satz 4 BayBG. Die Prüfung dieser Unterlagen durch kommunale Rechnungsprüfer dient Beihilfezwecken, sodass - unabhängig von einer Einwilligung des betroffenen Beamten - von einer grundsätzlichen Zulässigkeit der Weitergabe auszugehen ist, wobei das Verfassungsprinzip der Verhältnismäßigkeit, insbesondere der Erforderlichkeit der Weitergabe, gewahrt sein muss. Gegen eine stichprobenartige oder eine aus gegebenem Anlass durchgeführte Überprüfung der in den Akten verbleibenden Beihilfe**festsetzungen** habe ich daher nach wie vor keine Einwendungen.

13.2.3 Rechnungsprüfung und Personaldaten

Eine Kommune wollte von mir wissen, ob die Weitergabe der Namen der Bediensteten, die gegen die Benutzerrichtlinien zur Internetnutzung verstießen, an den Rechnungsprüfungsausschuss zulässig sei. Der Rechnungsprüfungsausschuss wollte die „Art der Verfehlungen“ aufgezeigt haben. Ich bin in meiner Stellungnahme davon ausgegangen, dass der Ausschuss daher nicht die

Namen dieser Personen oder andere personenbezogene Daten (Art. 4 Abs. 1 BayDSG) wissen wollte. Soweit sich also aus der Benennung der Verfehlungen kein Rückschluss auf bestimmte oder bestimmbare Personen ziehen lässt, stehen einer Mitteilung an den Rechnungsprüfungsausschuss keine datenschutzrechtlichen Bedenken entgegen.

Sollten personenbezogene Daten an den Rechnungsprüfungsausschuss übermittelt werden, steht dem, wie unter Nr. 13.2.1 ausgeführt, wegen Art. 17 Abs. 3 Satz 1 BayDSG jedenfalls der Zweckbindungsgrundsatz nicht entgegen.

Voraussetzung für ein zulässiges Nutzen personenbezogener Daten ist aber, dass dieses zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben **erforderlich** ist (Art. 17 Abs. 1 Nr. 1 BayDSG). Auch eine Nutzung innerhalb einer Stelle muss sich also am Grundsatz der Erforderlichkeit orientieren. Es ist also zu fragen, ob die Kenntnis konkreter Personen für die Aufgabenerfüllung des Rechnungsprüfungsausschusses erforderlich ist. Dies dürfte zumeist nicht der Fall sein, da es i.d.R. ausreicht, die **Art** der Verfehlungen ohne einen konkreten Personenbezug darzustellen. Sollte es für erforderlich gehalten werden, könnten die Verfehlungen nach nicht namentlich benannten Personen aufgeschlüsselt, also pseudonymisiert werden, so dass kein Rückschluss auf die Personen gezogen werden kann.

13.3 Kontrollbefugnisse des Arbeitgebers/Dienstherrn

13.3.1 Postöffnung in Behörden

Mit dieser Thematik habe ich mich bereits in meinem letzten (19.) Tätigkeitsbericht unter Nr. 12.2.1 beschäftigt. Die dort zitierte Allgemeine Dienstordnung (ADO) trat mit Ablauf des 31. Dezember 2000 außer Kraft. Seit dem 1. Januar 2001 ist die neue Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) in Kraft; Gemeinden, Landkreisen, Bezirken und sonstigen juristischen Personen des öffentlichen Rechts wird nach § 36 AGO empfohlen, nach dieser Geschäftsordnung zu verfahren. Die **Behandlung der Eingänge** ist nunmehr in § 12 AGO geregelt.

13.3.2 Erfassung der Telefondaten von Berufsgeheimnisträgern

Ein Krankenhaus hat bei mir angefragt, welche Aufzeichnungen bei einer Telefonanlage gemacht werden dürfen, die von Berufsgeheimnisträgern auch bei Gesprächen genutzt wird, die der Schweigepflicht unterfallen. Meine nachstehenden Ausführungen gelten nicht nur für Krankenhäuser, sondern für alle öffentliche Stellen, in denen Berufsgeheimnisträger - wie z. B. Berufspsychologen, Sozialarbeiter etc. (vgl. § 203 Abs. 1 StGB) - beschäftigt sind.

Zunächst verweise ich auf Nr. 17.1 meines 18. TB und die Bekanntmachung des Bayerischen Staatsministeriums der Finanzen zur „Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen“ (Dienstanschlussvorschriften-BayDAV; Bekanntmachung des Bayer. Staatsministeriums der Finanzen vom 07.11.1997, Nr. 63-H4700-1/418-73038, FMBl 1997, S. 280 ff.).

Die BayDAV bestimmt in Nr. 3.1.5, dass bei Verbindungen von Stellen, deren Telefonverkehr nicht der Aufsicht unterliegt und von Stellen, die im Rahmen einer freiwilligen Beratung tätig werden und damit einer **besonderen Verschwiegenheitspflicht** unterliegen, nur die Leistungsentgelte festzuhalten sind, sofern nicht diese Stellen eine Aufzeichnung oder Speicherung der übrigen Verbindungsdaten verlangen (siehe dazu aber unten). Führen Ärzte oder Träger anderer Berufsgeheimnisse im Rahmen der freiwilligen Beratung Telefongespräche, so muss die Telefondatenerfassung so ausgestaltet sein, dass ein unzulässiges Offenbaren von solchen Geheimnissen ausscheidet. Dem Dienstherrn/Arbeitgeber steht dann nicht das Recht zu, sich über außenstehende Telekommunikationsteilnehmer (B-Teilnehmer) zu informieren und Aufzeichnungen über die näheren Umstände der Telekommunikation zu machen, wenn besondere berufliche Verschwiegenheitspflichten es dem Beschäftigten verbieten, seinem Dienstherrn/Arbeitgeber Kenntnis über Personen zu verschaffen, mit denen er im Rahmen seiner Tätigkeit Kontakt hat (vgl. 18. TB, Nr. 17.1). Bereits die Identität einer solchen Person unterliegt der Schweigepflicht.

Diese rechtlichen Vorgaben müssen bei der Ausgestaltung einer Telefonanlage Berücksichtigung finden. Dies bedeutet, dass auch im Rahmen einer Überprüfung dienstlicher Gespräche verhindert werden muss, dass dem oder den Überprüfenden Geheimnisse bekannt werden, die Schweigepflichten unterliegen.

Zwar unterfällt nicht jedes dienstlich veranlasste Gespräch eines Geheimnisträgers automatisch der Schweigepflicht. So kann es sich z. B. um Gespräche handeln, in denen keine solchen Geheimnisse relevant werden (z. B. über organisatorische Fragestellungen) oder bei denen sich die der Schweigepflicht unterliegenden Tatsachen nur aus einer Kenntnis des Gesprächinhalts ergäben (z. B. Konsiliargespräch bei Ärzten). Daneben stehen aber die Gespräche, in denen die Schweigepflicht relevant ist. In diesen Fällen dürfen nur die Leistungsentgelte festgehalten werden (Nr. 3.1.5 BayDAV). Aus datenschutzrechtlicher Sicht dürfen selbst dann die übrigen Verbindungsdaten nicht aufgezeichnet werden, wenn dies die betroffenen Geheimnisträger verlangen (anders jedoch bis jetzt Nr. 3.1.5 der BayDAV), da diese Geheimnisse nicht zur freien Disposition des Geheimnisträgers stehen. Das Finanzministerium hat zugesagt, meine Rechtsauffassung bei der anstehenden Änderung der BayDAV zu berücksichtigen.

13.4 Informations- und Einsichtsrechte der Personalvertretung

Auch im Rahmen der vertrauensvollen Zusammenarbeit zwischen Dienststelle und **Personalvertretung** (vgl. Art. 2 Abs. 1 BayPVG) unterliegen die **Informations- und Einsichtsrechte** letzterer den datenschutzrechtlichen Bestimmungen. Zur Klarstellung weise ich auf Folgendes hin:

Die Personalvertretung ist nicht „Dritter“ im Sinne des Art. 4 Abs. 10 Satz 1 BayDSG, sondern Teil der „speichernden Stelle“ (vgl. Art. 4 Abs. 9 BayDSG) Dienststelle. Das bedeutet allerdings nicht, dass ihr schrankenlos Zugang zu sämtlichen in der Behörde verarbeiteten personenbezogenen Daten einzuräumen ist. Vielmehr ist jegliche Datennutzung (Art. 4 Abs. 7 BayDSG) an der spezialgesetzlichen Regelung (vgl. Art. 2 Abs. 7 BayDSG) des Art. 69 Abs. 2 BayPVG oder den einschlägigen gesetzlichen Bestimmungen, z. B. bei der Forderung auf Einsichtnahme in automatisiert gespeicherte Personalaktendaten an Art. 100 h Abs. 1 Satz 1 BayBG, zu messen.

Nach Art. 69 Abs. 2 Satz 1 BayPVG ist der Personalrat **zur Durchführung seiner Aufgaben** rechtzeitig und umfassend zu unterrichten. Ein Anspruch der Personalvertretung auf umfassende und rechtzeitige Information besteht aber nur insoweit, als sie Auskünfte und dergleichen von Seiten der Dienststelle benötigt, um die ihr obliegenden Aufgaben erfüllen und ihre Beteiligungsrechte rechtzeitig und uneingeschränkt wahrnehmen zu können. Gemäß Art. 69 Abs. 2 Satz 2 BayPVG sind dem Personalrat die hierfür erforderlichen Unterlagen zur Verfügung zu stellen. Er ist daher verpflichtet, bei Inanspruchnahme seines Informationsrechts den Dienststel-

lenleiter jeweils darüber zu unterrichten, aus welchem bestimmten Anlass er die Vorlage welcher Unterlagen verlangt und aus welchen Gründen er dies zur Erfüllung seiner Aufgaben für erforderlich hält, soweit sich die Notwendigkeit der Information nicht schon aus der Sache selbst ergibt. Die Personalvertretung ist also kein Kontrollorgan der Verwaltung, das die Aufgabenerfüllung und den inneren Betrieb der Dienststelle allgemein zu überwachen hat.

Im Übrigen ist die Personalvertretung (Personalrat oder Stufenvertretung) nicht im Sinne von Art. 100 a Abs. 3 BayBG „mit der Bearbeitung von Personalangelegenheiten beauftragt“. Nach Art. 69 Abs. 2 Satz 4 BayPVG dürfen Personalakten nur mit schriftlicher Zustimmung des Beschäftigten und nur von einem von ihm bestimmten Mitglied des Personalrats eingesehen werden. Von dienstlichen Beurteilungen ist nur die abschließende Bewertung bekannt zu geben, Art. 69 Abs. 2 Satz 3 BayPVG.

14 Gewerbe und Handwerk

14.1 Änderung der Gewerbeordnung

Im Berichtszeitraum wurde die Gewerbeordnung geändert (Drittes Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 24.08.2002 BGBl. I S. 3412). Aus datenschutzrechtlicher Sicht sind insbesondere folgende Neuregelungen von Bedeutung:

Durch eine Änderung des § 11 Abs. 5 und 6 GewO wurden bisher bestehende Einschränkungen bei der Übermittlung personenbezogener Daten aufgehoben und die Anwendbarkeit der Datenschutzgesetze der Länder auch für Datenübermittlungen gesetzlich geregelt. Damit ist nach der Gesetzesbegründung einem Bedürfnis der Praxis Rechnung getragen worden. In der Gesetzesbegründung wird dazu beispielhaft darauf hingewiesen, dass eine Gewerbebehörde, die bei der Erfüllung ihrer Aufgaben erfährt, dass ein Berufskraftfahrer nicht mehr fahrtauglich ist, die Fahrerlaubnisbehörde nach der bisherigen Rechtslage darüber nicht unterrichten durfte. Aufgrund der Änderung des § 11 Abs. 6 GewO sei nunmehr eine Rechtsgrundlage für die Informati-

on der Fahrerlaubnisbehörde gegeben. Die Neufassung entspreche auch der vergleichbaren Regelung des § 9 Abs. 6 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern.

Nach dem neuen § 14 Abs. 1 a GewO teilen die Finanzbehörden den zuständigen Behörden den Namen und die Anschrift der Gewerbetreibenden mit, die ihr Gewerbe beim Finanzamt abgemeldet haben. Mitgeteilt wird auch der Tag, an dem die Steuerpflicht endete. Die Mitteilungspflicht besteht nicht, soweit ihre Erfüllung mit einem unverhältnismäßigen Aufwand verbunden wäre. In der Gesetzesbegründung wird zu dieser Neuregelung darauf hingewiesen, dass Gewerbetreibende in vielen Fällen die Beendigung ihrer selbstständigen Tätigkeit nur bei dem für sie zuständigen Finanzamt abmelden, um künftige steuerliche Verpflichtungen, insbesondere Steuererklärungspflichten, zu vermeiden. Dem Gebot des § 14 GewO zur Abmeldung bei der Gewerbebehörde würden sie demgegenüber häufig nicht nachkommen. Da die Finanzämter somit in der Regel diesbezüglich über bessere Informationen verfügen würden, sollen sie diese künftig auch den Gewerbebehörden übermitteln, sofern dies mit keinem unverhältnismäßigem Aufwand verbunden sei. In Betracht würden hierbei insbesondere automationsgestützte Mitteilungen ggf. auch in elektronischer Form, kommen.

Im 19. Tätigkeitsbericht 2000 habe ich unter der Nr. 13.1 darauf hingewiesen, dass nach der damals geltenden Fassung des Art. 14 Abs. 7 Satz 1 GewO Daten aus den Gewerbeanzeigen zwar innerhalb der jeweiligen Gemeinde, nicht aber auch innerhalb des Landratsamtes weitergeleitet werden dürfen. Im Ergebnis kam danach 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 Satz 1 i.V.m. Abs. 6 GewO zulässig war. 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, habe ich keine Bedenken gegen eine Ergänzung des § 14 Abs. 7 GewO mit dem Ziel vorgetragen, die Datenweitergabe auch innerhalb des Landratsamtes unter den in § 14 Abs. 6 GewO genannten Voraussetzungen zu gestatten. Der Gesetzgeber hat inzwischen reagiert und § 14 Abs. 7 Satz 1 GewO so gefasst, dass nunmehr auch eine Datenweitergabe innerhalb des Landratsamtes zulässig ist.

Das Gesetz tritt am 01.01.2003 in Kraft.

14.2 Bundeseinheitliche und behördenübergreifende Wirtschaftsnummer

Die Bundesregierung plant für das Jahr 2005 die Einführung einer einheitlichen Wirtschaftsnummer für Unternehmen, Betriebe und sonstige wirtschaftlich Tätige. Diese Nummer soll bestehende Nummernsysteme ersetzen und im Verkehr mit Behörden zur Bezeichnung und Identifizierung des wirtschaftlich Tätigen verwendet werden. Mit der Nummer soll ein Datensatz verknüpft werden, der die Grunddaten eines wirtschaftlich Tätigen enthält (dessen „Stammdaten“). Damit erhalten die Behörden die Möglichkeit, die aktuellen Stammdaten mit den in ihrer Zuständigkeit bereits erhobenen Daten zu verknüpfen. Die Vergabe der Wirtschaftsnummer und die Pflege des Stammdatensatzes soll durch eine zentrale Stelle erfolgen. Die Bundesregierung sieht in der einheitlichen Wirtschaftnummer erhebliche Vorteile sowohl für die wirtschaftlich Tätigen als auch für die Verwaltung. Der Umfang der Dateneingabe und -anfrage werde sich verringern, Unternehmen würden in großem Umfang von Meldungen und damit von bürokratischen Hemmnissen entlastet. Da die bei Behörden vorhandenen Informationen mangels eindeutigem Identifikationsmerkmal oftmals nicht eindeutig zugeordnet werden könnten, seien Verknüpfungen von Daten nicht immer möglich. Damit bestehe die Gefahr, dass die Datenbanken mancher Verwaltungen nicht fehlerfrei und nicht auf dem neuesten Stand sind. Vor der bundesweiten Einführung soll die zentrale Vergabe und Pflege der Wirtschaftsnummer sowie des damit verbundenen Stammdatensatzes vorab getestet werden. Dazu hat der Bundestag mit Zustimmung des Bundesrates das Gesetz zur Vorbereitung einer bundeseinheitlichen Wirtschaftsnummer vom 22. Mai 2002 (WiNuEG) beschlossen (BGBl. I S. 1644). Die Erprobung wird durch die Bundesanstalt für Arbeit durchgeführt, die auch zentrale Vergabe- und Speicherstelle sein wird.

Die Einführung der bundeseinheitlichen Wirtschaftsnummer ist datenschutzrechtlich von Bedeutung, da sie auch natürlichen Personen zugeteilt wird, soweit diese wirtschaftlich tätig sind und die Voraussetzungen des § 3 WiNuEG erfüllen. In der Gesetzesbegründung wird im Allgemeinen Teil unter der Nr. 6 zum Bereich Datenschutz u. a. ausgeführt, mit dem für die Erprobung vorgesehenen Verfahren, welches Grundlage für das spätere Gesetz sei, werde erreicht, dass

- die Datenverarbeitung der beteiligten Behörden nicht ausgeweitet sondern lediglich die Erhebung und Pflege bestimmter, in allen Zweigen der Wirtschaftsverwaltung geführter

Grunddaten vereinfacht wird;

- die Informationsbeziehungen zwischen den Verwaltungen vereinfacht werden, die Daten aber keineswegs zusammengeführt werden dürfen;

- die Nutzung der Wirtschaftsnummer derartig begrenzt wird, dass sie sich für die auch in erheblichem Umfang betroffenen natürlichen Personen, wie z. B. freiberuflich Tätigen, nicht zu einem allgemeinen Personenkennzeichen entwickeln kann;

- die amtliche Statistik an der Entwicklung der Struktur der Wirtschaftsnummer beteiligt wird, ohne zum Datenlieferanten für die Wirtschaftsverwaltung zu werden.

Aus datenschutzrechtlicher Sicht ist besonders darauf zu achten, dass die bundeseinheitliche Wirtschaftsnummer nicht die Funktion eines Personenkennzeichens erhält. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil vom 15. Dezember 1983 unmissverständlich zum Ausdruck gebracht, dass die Verknüpfung der bei den verschiedenen Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbestände oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal und damit die Erstellung von Persönlichkeitsprofilen der Bürger durch die Zusammenführung von Daten aus verschiedenen Lebensbereichen unzulässig wäre. Die bundesweite und behördenübergreifende Wirtschaftsnummer erfasst die betroffenen natürlichen Personen „nur“ in einem bestimmten Lebensbereich, nämlich ihrer wirtschaftlichen Betätigung. Aus diesem Grund und bei Beachtung der o. g. Einschränkungen (keine Ausweitung der Datenverarbeitung der beteiligten Behörden, keine Zusammenführung der Datenbestände der betroffenen Verwaltungen und Begrenzung der Nutzung der Wirtschaftsnummer zur Pflege der Stammdaten durch die beteiligten Behörden) hat die Wirtschaftsnummer nach meinem Dafürhalten nicht die Funktion eines unzulässigen Personenkennzeichens.

Nach § 3 Abs. 1 Nr. 2 WiNuEG erhalten auch alle Personen, für die nach den Vorschriften des Dritten Abschnitts des SGB IV eine Meldepflicht besteht, eine Wirtschaftsnummer. Davon werden alle privaten Haushalte, die eine Haushaltshilfe beschäftigen, erfasst. Es mag zwar von der Zielvorstellung her, möglichst viele Nummernsysteme zu ersetzen, sinnvoll sein, auch die Betriebsnummer nach § 28 a Abs. 8 SGB IV durch die Wirtschaftsnummer zu ersetzen. Aus datenschutzrechtlicher Sicht habe ich jedoch Bedenken gegen die Einbeziehung der Personen, die eine

Haushaltshilfe beschäftigen, in den Kreis der Beteiligten, die eine einheitliche Wirtschaftsnummer erhalten, weil im Gegensatz zu herkömmlichen Wirtschaftseinheiten, deren Tätigwerden vielfältiger staatlicher Kontrolle unterliegt, Dienstleistungen im Haushaltsbereich der Privatsphäre zuzuordnen sind. Weder das Lehrerehepaar noch der Rentner, die eine Haushaltshilfe beschäftigen, werden im herkömmlichen Sinn als wirtschaftlich Tätige betrachtet. Ich lehne die Vergabe einer Wirtschaftsnummer an diesen Personenkreis daher ab.

Meine datenschutzrechtlichen Forderungen bringe ich in die Schwerpunktgruppe „Datenschutz“ ein, die zur fachlichen Beratung des Beirats nach § 12 WiNuEG eingerichtet wurde. Der Beirat begleitet unter Federführung des Bundesministeriums für Wirtschaft und Technologie und des Freistaates Bayern die Erprobung der Wirtschaftsnummer.

14.3 Prüfung des Verfahrens „GEWAN“

Im Berichtszeitraum habe ich das Verfahren Gewerbeanzeigen im Netz (GEWAN) überprüft, das vom Bayerischen Landesamt für Statistik und Datenverarbeitung entwickelt wurde. Das Verfahren soll den Kommunen elektronische Unterstützung bei der Erfassung und Pflege von Gewerbeanzeigen (An-, Ab- und Ummeldung) bieten. Darüber hinaus soll das Verfahren die elektronische Übermittlung von Daten aus der Gewerbeanzeige an die am sog. Verständigungsdienst beteiligten Stellen (Industrie- und Handelskammer, Handwerkskammer, Gewerbeaufsichtsamt, Eichamt, Landesverband Bayern und Sachsen der gewerblichen Berufsgenossenschaft, Registergericht, Statistisches Landesamt, Arbeitsamt, Finanzamt und die Allgemeine Ortskrankenkasse) ermöglichen. Die Gewerbeanzeigen sind gemäß § 14 Abs. 4 Satz 1 der Gewerbeordnung (GewO) auf den drei Vordrucken für die Gewerbean-, um- und -abmeldung zu erstatten, deren Form und Inhalt durch § 14 Abs. 4 i.V.m. den Anlagen GewA1 bis 3 zur Gewerbeordnung festgelegt ist. Grundlage für den sog. Verständigungsdienst ist § 14 Abs. 5 und Abs. 8 a GewO sowie § 138 der Abgabenordnung (AO). Nach Ziffer 6.3.2 der in Bayern geltenden *Allgemeinen Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewo* (GewAnzVwV) ist die elektronische Datenübermittlung auf der Grundlage der einheitlichen Datensatzbeschreibung, die das Statistische Bundesamt zur Verfügung stellt, ausdrücklich zugelassen. Durch das Dritte Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 24. August 2002, das am 1. Januar 2003 in Kraft tritt, wurde zwischenzeitlich im Gesetzestext selbst durch einen neu eingeführten Satz 3 klargestellt, dass die zuständige Behörde Abweichun-

gen von der Form, nicht aber vom Inhalt der Anzeige zur elektronischen Datenverarbeitung zulassen kann.

Die von mir geprüfte Version GEWAN 3.x ist seit Mai 2001 in den Gewerbeämtern einiger Gemeinden und kreisfreier Städte sowie bei einigen Landratsämtern im Einsatz. Der Sachbearbeiter vor Ort benötigt dazu einen browserfähigen Computer, da alle Programme zentral auf dem Server beim Bayerischen Landesamt für Statistik und Datenverarbeitung gespeichert sind. Der zentrale Server verständigt automatisch medienbruchfrei die nach der Gewerbeordnung empfangsberechtigten Stellen, so dass das bisherige Versenden der (Papier-)Durchschläge sowie das Neuerfassen der Gewerbedaten in diesen Dienststellen entfällt. Mit Hilfe eines sog. lernenden Thesaurus ist GEWAN in der Lage, den gemeldeten Tätigkeiten weitgehend automatisch einen fünfstelligen Schlüssel gemäß der bundesweit gültigen Wirtschaftszweigsystematik WZ93 zuzuordnen (sog. Signierung). Dadurch sind statistische Vergleiche der Gewerbedaten auf kommunaler, nationaler und europäischer Ebene möglich.

Das Bayerische Landesamt für Statistik und Datenverarbeitung hatte mich bereits während der Anfangsphase des Projekts im Jahr 1997 ausführlich über die Konzeption und Planungen zu GEWAN informiert. Meine nachfolgend genannten Anforderungen an das Projekt aus der Sicht des Datenschutzes konnten dadurch von Anfang berücksichtigt werden: Durch die Forderung, dass die Daten aus den Gewerbeanzeigen auf dem Rechner des Landesamtes logisch getrennt für die einzelnen Gemeinden gespeichert werden, soll vor allem sichergestellt werden, dass *kein* zentrales (und datenschutzrechtlich unzulässiges) Register aller in Bayern gemeldeten Gewerbe entsteht. Weiterhin habe ich gefordert, dass sowohl organisatorisch als auch physikalisch streng zwischen der Funktion des Landesamtes als Empfänger der Daten im Verständigungsdienst und seiner Funktion als Verfahrensbetreuer für GEWAN unterschieden wird. Das Landesamt verpflichtete sich, gegenüber den Gemeinden vertraglich zuzusichern, dass keine Daten an Dritte weitergegeben werden und dass keine Auswertungen vorgenommen werden. Durch entsprechende Datensicherungsmaßnahmen beim Landesamt soll insbesondere gewährleistet werden, dass die Gemeinden und Landratsämter nur auf die jeweils eigenen Daten zugreifen können. Darüber hinaus sollen Maßnahmen zur Sicherung der Integrität, Vertraulichkeit und Zurechenbarkeit (Authenzität) der übertragenen Daten getroffen und durch den Einsatz einer hochwertigen Verschlüsselungstechnik für eine sichere Übertragung der Daten gesorgt werden. Ein unberechtigter Zugang zum als auch ein unberechtigter Zugriff auf den zentralen GEWAN-Server beim Landesamt sollte verhindert werden.

Meine rechtliche und technische Überprüfung der Einhaltung des Datenschutzes bei GEWAN im Oktober 2001, die ich sowohl beim Bayerischen Landesamt für Statistik und Datenverarbeitung als auch bei einer Gemeinde vor Ort durchgeführt habe, hat ergeben, dass bei der Umsetzung des Verfahrens in die Praxis meinen o. g. datenschutzrechtlichen sowie grundsätzlichen unmittelbar verfahrensbezogenen technisch-organisatorischen Forderungen Rechnung getragen wurden. Die Umsetzung einiger von mir geforderter, aber nur innerhalb des LfStaD relevanter, technisch-organisatorischer Maßnahmen konnte bis zum Redaktionsschluss nicht abgeschlossen werden. Das LfStaD arbeitet weiter daran.

Der im Konzept von GEWAN vorgesehene automatische Verteilerdienst über verschlüsselte E-Mail konnte zum Prüfungszeitpunkt weder in Test-, noch in Echtbetrieb untersucht werden, da dieser erst in einer späteren Phase testweise mit einigen wenigen Empfängern erprobt werden sollte. Laut Auskunft des Statistischen Landesamtes wird eine regelmäßige Erprobung des automatischen Verteilerdienstes seit Anfang des Jahres 2002 mit dem überwiegenden Teil der am Verständigungsdienst beteiligten Stellen durchgeführt. Inzwischen sind zwei dieser Stellen aus der Erprobungsphase in den Echtbetrieb gewechselt. Die datenschutzrechtliche Überprüfung des automatischen Verteilerdienstes über verschlüsselte E-Mail behalte ich mir vor.

Die Bereitstellung des zentralen Servers durch das Bayerische Landesamt für Statistik und Datenverarbeitung und seine Funktion als Verfahrensbetreuer für GEWAN stellt eine Auftragsverarbeitung im Sinne des Art. 6 BayDSG dar. Gemäß Art. 6 Abs. 2 Satz 2 BayDSG ist der Auftrag zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag schriftlich zu erteilen. Da nach Auskunft des Bayerischen Landesamtes für Statistik und Datenverarbeitung zum Prüfungszeitpunkt keine (schriftlichen) Vereinbarungen mit den Gemeinden (Auftraggeber) über die Auftragsdatenverarbeitung gemäß Art. 6 BayDSG durch das Landesamt (Auftragnehmer) vorlagen, habe ich das Landesamt aufgefordert, die schriftliche Erteilung des Auftrags umgehend nachzuholen. Dazu hat mir das Statistische Landesamt mitgeteilt, dass zwischenzeitlich mit allen Neukunden schriftliche Vereinbarungen gemäß Art. 6 Abs. 2 Satz 2 BayDSG abgeschlossen werden. Bei den Altkunden wird die schriftliche Erteilung des Auftrags bis zum Ende des Jahres 2002 nachträglich eingeholt.

15 Statistik

15.1 Datenschutz im Rahmen der Gehalts- und Lohnstrukturerhebung 2001

Mehrere Bürger haben sich im Zusammenhang mit der vom Landesamt für Statistik und Datenverarbeitung durchgeführten Gehalts- und Lohnstrukturerhebung 2001 an mich gewandt. Sie brachten vor, von ihrem jeweiligen Arbeitgeber darüber informiert worden zu sein, dass dieser auf Grund der Anforderung des Landesamtes eine Vielzahl von Daten seiner Arbeitnehmer wie bspw. vollständiger Name, Geburtsdatum, Steuerklasse, Bruttogehalt, Angaben zu den Beiträgen zur Sozial- und Krankenversicherung usw. zu übermitteln habe. Die betroffenen Bürger sahen in der mangelnden Anonymität einen Verstoß gegen datenschutzrechtliche Bestimmungen. Nach Prüfung der Rechtslage ergibt sich Folgendes:

Nach § 1 Abs. 1 Nr. 3 Lohnstatistikgesetz wird in unregelmäßigen Abständen (aktuell für das Berichtsjahr 2001) eine Statistik über die Struktur der Arbeitsverdienste und Arbeitszeiten sowie über die Arbeitskosten durchgeführt. Die Statistik wird in Form einer Stichprobenerhebung durchgeführt.

Die Erhebungsmerkmale der Statistik sind in § 7 und § 9 des Gesetzes definiert. Hier werden eine Vielzahl von Merkmalen, u.a. die bereits erwähnten Daten abgefragt. Bei der Angabe der Art der ausgeübten Tätigkeit kann die auch gegenüber dem Sozialversicherungsträger in verschlüsselter Form gemeldete Berufsbezeichnung verwendet werden. Dabei handelt es sich aber nicht um die Sozialversicherungsnummer.

§ 11 des Gesetzes definiert die Hilfsmerkmale der Erhebung. Hilfsmerkmale dienen der technischen Durchführung der Statistik. Sie sind nach Abschluss der Überprüfung auf Schlüssigkeit und Vollständigkeit zu löschen. Das Lohnstatistikgesetz bestimmt in diesem Zusammenhang, dass der Arbeitgeber bei Lieferung der Erhebungsmerkmale eines jeden einzubeziehenden Arbeitnehmers eine betriebliche Kennziffer des Arbeitnehmers zu liefern hat. Diese dient bei Rückfragen zu ggf. unplausiblen Angaben zur Identifikation des Falles. Der Arbeitgeber ist bei Vergabe dieser betrieblichen Kennziffer frei. Nur wenn eine betriebliche Kennziffer nicht vorhanden

ist, kann als Hilfsmerkmal auch der Name des einzubeziehenden Arbeitnehmers verwendet werden. In diesem Fall sind die Betroffenen vom Arbeitgeber über die Erhebung zu unterrichten.

Ziel und Zweck der Statistik ist nicht die personenbezogene Aufbereitung bestimmter Erhebungsmerkmale. Die (hilfsweise) Lieferung des Namens soll nur evtl. erforderliche Rückfragen ermöglichen. Die Namensangabe kann durch den Arbeitgeber auch vermieden werden.

Festzuhalten ist darüber hinaus, dass - selbst bei namentlicher Datenübermittlung - die Bediensteten des Statistischen Landesamtes an die statistische Geheimhaltung gem. § 16 Bundesstatistikgesetz gebunden sind. Erkenntnisse über Verstöße gegen diese Geheimhaltungsvorschrift lagen und liegen mir nicht vor.

Ich musste den Bürgern deshalb mitteilen, dass aus den genannten Gründen gegen die angesprochene statistische Erhebung aus datenschutzrechtlicher Sicht keine Einwendungen erhoben werden können. Meiner Ansicht nach wäre es wünschenswert, wenn die Arbeitgeber die Datenlieferung über die im Gesetz vorgesehene betriebliche Kennziffer abwickeln.

16 Schulen und Hochschulen

16.1 Schulen

16.1.1 Ergänzungen des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG)

Nach dem Massaker an einer Schule in Erfurt schlug das Bayerische Staatsministerium für Unterricht und Kultus vor, das BayEUG durch Regelungen über die Möglichkeit oder Pflicht zur Information der **früheren** Erziehungsberechtigten volljähriger Schüler über Ordnungsmaßnahmen und ein auffallendes Absinken des Leistungsstandes und sonstige wesentliche, den Schüler betreffende Vorgänge zu ergänzen.

Im Rahmen meiner datenschutzrechtlichen Beurteilung wies ich darauf hin, dass entsprechende Vorschriften in das Recht volljähriger Schüler auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreifen. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts gewährleistet das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Dies gilt mit Erreichen der Volljährigkeit grundsätzlich auch gegenüber den Eltern. Beschränkungen dieses Rechts sind nur im überwiegenden öffentlichen Interesse auf der Grundlage einer (verfassungsmäßigen) gesetzlichen Regelung zulässig. Ein solches überwiegendes öffentliches Interesse kann jedenfalls mit dem Personensorgerecht der Eltern nicht begründet werden, da das in Art. 6 Abs. 2 Satz 1 GG statuierte Recht der Eltern auf Pflege und Erziehung der Kinder mit fortschreitendem Alter des Kindes abnimmt und mit der Volljährigkeit erlischt. Ich hielt es jedoch für vertretbar, ein solches überwiegendes Allgemeininteresse damit zu begründen, dass der Erziehungs- und Bildungsauftrag der Schule, der nicht mit Eintritt der Volljährigkeit endet, grundsätzlich besser zu erfüllen ist, wenn die Möglichkeit zur Unterrichtung der Eltern auch volljähriger Schüler gegeben ist. Ich bin dabei davon ausgegangen, dass ein Gespräch mit den Eltern auch bei volljährigen Schülern zur Lösung von schweren Konfliktsituationen beitragen kann.

Ich habe aber meine Bedenken gegen eine **Informationspflicht** der Schulen in allen Fällen - ohne Rücksicht auf die konkreten Verhältnisse im Einzelfall - und in Bezug auf alle Ordnungsmaßnahmen zum Ausdruck gebracht. Eine solche Verpflichtung in allen Fällen halte ich mit dem auch für den Gesetzgeber geltenden Grundsatz der Verhältnismäßigkeit nicht für vereinbar. Dies gilt umso mehr, wenn ein Widerspruchsrecht volljähriger Schüler gegen die Unterrichtung nicht vorgesehen ist.

Ich habe zu den beabsichtigen Regelungen im Ausschuss für Bildung, Jugend und Sport Stellung genommen und dem Ausschuss für Verfassungs-, Rechts- und Parlamentsfragen einen eigenen Vorschlag für eine Gesetzesformulierung übermittelt, nachdem im Zuge der Beratungen im Ministerrat die Regelungen auf volljährige Schüler, welche das 21. Lebensjahr noch nicht vollendet haben, begrenzt wurden. Mein Vorschlag sah eine **Kann-bestimmung** zur Information nur bei schwereren Ordnungsmaßnahmen und ein Widerspruchsrecht des Schülers vor, über das er schriftlich mit Eintritt der Volljährigkeit oder bei Eintritt in die Schule zu informieren sei.

Der am 01. August 2002 in Kraft getretene Art. 88 a BayEUG regelt nunmehr, dass frühere Erziehungsberechtigte volljähriger Schüler, welche das 21. Lebensjahr noch nicht vollendet haben, über die schweren Ordnungsmaßnahmen nach Art. 86 Abs. 2 Nr. 3 bis 10 BayEUG (Versetzung in eine andere Klasse bis Ausschluss von allen Schulen auch mehrerer Schularten) unterrichtet werden sollen. Vergleichbares gilt gemäß Art. 75 Satz 2 BayEUG bei einem auffallenden Absinken des Leistungsstands und sonstigen wesentlichen, den Schüler betreffenden Vorgängen.

Aus datenschutzrechtlicher Sicht begrüße ich, dass die Unterrichtungsmöglichkeiten auf schwerere Ordnungsmaßnahmen eingeschränkt wurden und die Regelung keine Unterrichtungspflicht mehr enthält. In die Auslegung der **Soll-Bestimmung** können z. B. auch pädagogische Überlegungen (besondere Situation in der Familie etc.) einfließen, die gegen eine Information in diesen Fällen sprechen. Ich bedauere es jedoch, dass ein Widerspruchsrecht volljähriger Schüler gegen die Unterrichtung nicht mehr vorgesehen ist. Für selbstverständlich halte ich es, dass der Schüler oder die Schülerin von der Absicht die Eltern zu verständigen unterrichtet wird.

16.1.2 Neufassung der „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“

Die **„Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“** (KMBek vom 19.04.2001) wurden unter meiner Beteiligung mit Wirkung vom 1. Juni 2001 neu gefasst und im KWMBl I S. 112 veröffentlicht. Ich bitte die Schulen um Beachtung.

Insbesondere wurden in Anlehnung an Nr. 15.1 meines 19. Tätigkeitsberichts Konkretisierungen zu Veröffentlichungen in der Homepage und im Jahresbericht einer Schule (Nr. 4.4 Buchstaben d und e) aufgenommen.

So ist nunmehr in dieser Bekanntmachung festgehalten, dass vor der Einstellung personenbezogener Daten in das Internet die Einwilligung der Betroffenen einzuholen ist. Ferner wurde sie dahingehend ergänzt, dass die Aufnahme von Fotos in den Jahresbericht und in die Homepage, aber auch die Weitergabe von Fotos an die Presse die Einwilligung des Betroffenen erfordert.

Zwischenzeitlich wurden diese „Erläuternden Hinweise“ vom Bayerischen Staatsministerium für Unterricht und Kultus mit Bekanntmachung vom 10.10.2002 (KWMBl I S. 354) aufgrund der in

den Nrn. 16.1.5 und 16.1.6 dieses Tätigkeitsberichts geschilderten Vorfälle auf meine Anregung hin mit sofortiger Wirkung in den Nrn. 4.4 Buchstabe d und 4.6 dahingehend geändert, dass von der Einholung der Einwilligung in Aufnahme von Schüleradressen in die Jahresberichte abgesehen werden soll. Weiter wurde in Bezug auf die Erstellung von Schülerausweisen auf das Muster für einen Vertrag zur Auftragsdatenverarbeitung auf meine Homepage hingewiesen (www.datenschutz-bayern.de/Technik/Orientierungshilfen/Mustervorlagen.html).

16.1.3 „Schulen ans Netz“

Im Zuge der Weiterentwicklung der Informations- und Kommunikationsgesellschaft gehört auch das Lernen am PC und mit Hilfe des Internets in allen Fächern zum Unterrichtsalltag. Das Bayerische Staatsministerium für Unterricht und Kultus hat deshalb im Herbst letzten Jahres die **Lehrerfortbildung „Intel - Lehren für die Zukunft“** gestartet. Leider wurde ich nicht bereits im Vorfeld in das von der Fa. Intel initiierte bundesweite Fortbildungskonzept zur Lehrerweiterbildung einbezogen, was ich ausdrücklich bemängle. Da ich aber von meinem saarländischen Kollegen rechtzeitig darauf aufmerksam gemacht wurde, konnte ich noch an das Ministerium herantreten und meine Anregungen einbringen.

So hat die Akademie für Lehrerfortbildung in Dillingen am 4./5. Oktober 2001 einen Redaktionslehrgang durchgeführt, bei dem ich auch vertreten war. In der Lehrerfortbildungsbroschüre „Intel - Lehren für die Zukunft“ sowie in einer beiliegenden CD sollen zukünftig auch datenschutzrechtliche Zielsetzungen Berücksichtigung finden. Insbesondere sollen Hinweise auf die Risiken des Internets, auf technisch-organisatorische Sicherheitsmaßnahmen sowie Verweise auf datenschutzrechtliche Bestimmungen (z. B. Art. 85 BayEUG und die Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes) aufgenommen werden.

16.1.4 Videoüberwachung in Schulen

Aufgrund aktueller Ereignisse erhielt ich mehrere Anfragen zur Zulässigkeit der **Videoüberwachung in Schulen** (vgl. auch Ziffer 17.3.2). Ferner berichteten einige Zeitungen über derartige Maßnahmen. Das Bayer. Staatsministerium für Unterricht und Kultus hat zwischenzeitlich die Regierungen und die Ministerialbeauftragten mit KMS vom 02.09.2002 (Nr. III/1-S4310/1-6/87

188) über die im Einvernehmen mit mir festgelegten Grundsätze für die Zulässigkeit der Videoüberwachung informiert und damit die Bitte verbunden, die Schulen hiervon zu unterrichten.

Zur Videoüberwachung öffentlicher Plätze durch Kommunen hatte ich mich bereits in Nr. 8.8 meines 19. Tätigkeitsberichts geäußert. Eine Videoüberwachung einzelner Bereiche einer Schule, wie beispielsweise des Eingangsbereichs, zum Schutz der Schüler oder Lehrer und damit zur Gefahrenabwehr, überschreitet den Rahmen einer im Sinne des Art. 85 Abs. 1 Satz 1 BayEUG zulässigen Datenerhebung grundsätzlich nicht.

Allerdings muss auch auf dem Schulgelände und in den Schulräumen grundsätzlich die Möglichkeit und das Recht bestehen, sich frei und unbeobachtet bewegen zu können. Dieses schutzwürdige Interesse wird durch eine Videoüberwachung berührt. Daher ist eine Überwachung räumlich auf diejenigen Bereiche zu begrenzen, die unter Beachtung des Grundsatzes der Verhältnismäßigkeit für diese Sicherheitsmaßnahme effektiv erscheinen.

Gemäß Art. 85 Abs. 1 Satz 3 BayEUG i. V. m. Art. 16 Abs. 2 Satz 1 BayDSG sind personenbezogene Daten primär beim Betroffenen mit dessen Kenntnis zu erheben. Auf die Videoüberwachung ist deshalb durch Hinweisschilder aufmerksam zu machen, auf denen der Erhebungszweck anzugeben ist (vgl. Art. 16 Abs. 3 Satz 1 BayDSG). Da in aller Regel datenschutzrechtlich nicht unbedingt einsichtsfähige Minderjährige betroffen sind, sind die Erziehungsberechtigten über die Videoüberwachung in geeigneter Form (schriftlich) zu unterrichten. Eine entsprechende Information aller Erziehungsberechtigten (z. B. mittels Elternbrief) ist auch deshalb angebracht, weil auch Erziehungsberechtigte und sonstige Personen von der Videoüberwachung betroffen sein können.

Die Aufzeichnungen dürfen nur zur Täterfeststellung und/oder zur Beweissicherung ausgewertet werden. Sie sind zu löschen, sobald sie hierzu nicht mehr erforderlich sind. Werden **maximal drei Schultage** nach der jeweiligen Aufzeichnung keine Auffälligkeiten festgestellt, sind die Aufzeichnungen ohne Auswertung zu löschen. Bei festgestellten Auffälligkeiten ist sicherzustellen, dass die Aufzeichnungen gelöscht werden, sofern sie für die notwendigen Beweisführungen nicht mehr erforderlich sind. Die Aufzeichnungen sind zudem gegen unberechtigte Zugriffe zu sichern.

Bezüglich der Lehrkräfte und der sonstigen Beschäftigten, die sich ebenfalls in dem videoüberwachten Bereich aufhalten bzw. diesen durchqueren, ist auf die Mitbestimmung des Personalrats nach Art. 75 a Abs. 1 Nr. 1 BayPVG hinzuweisen.

Allgemein halte ich nach wie vor eine Aufsicht durch Personen (z. B. Lehrer, Hausmeister) oder andere präventive Maßnahmen (wie z. B. die Einrichtung einer Pforte) aus datenschutzrechtlicher Sicht für angemessener als eine automatisierte Überwachung durch Videokameras, verkenne aber den mit der Stellung von Aufsichtspersonen einhergehenden kostenintensiven und zeitlichen Aufwand nicht. Die angestrebte Abschreckung und mögliche Täterfeststellung lässt gleichwohl die Einrichtung von Videokameras unter den geschilderten Voraussetzungen als datenschutzrechtlich zulässig erscheinen.

16.1.5 Zulässige Daten im Jahresbericht einer Schule

Im Berichtzeitraum wurde mir bekannt, dass im Jahresbericht einer bayerischen Schule bei den (meisten) Schülern der Abschlussklassen deren Wohnadresse (Wohnort und Straße) aufgeführt wurde. Auf meine Anfrage teilte der Schulleiter mit, dass die Adressen der Abschlussschüler mit deren Einwilligung abgedruckt worden seien. Bei Schülern, die dies nicht wünschten, sei die Adresse nicht veröffentlicht worden.

Der Abdruck der Wohnadressen von Schülern in den Jahresberichten ist unzulässig, so dass ich dies beanstandet habe. Gemäß Art. 85 Abs. 3 BayEUG dürfen nämlich im Jahresbericht einer Schule (nur) folgende personenbezogene Daten enthalten sein: „Name, Geburtsdatum, Jahrgangsstufe und Klasse der Schüler, Name, Fächerverbindung und Verwendung der einzelnen Lehrkräfte, Angaben über besondere schulische Tätigkeiten und Funktionen einzelner Lehrkräfte, Schüler und Erziehungsberechtigter“. Ich halte diese Aufzählung für abschließend. Aus dem Kommentar von Amberg/Falckenberg/Stahl, Das Schulrecht in Bayern, ergibt sich, dass weitere personenbezogene Daten, wie z. B. die Bekenntniszugehörigkeit der Schüler oder Lehrkräfte, Angaben über Anschrift oder Geburtsort der Schüler, sowie der Beruf der Erziehungsberechtigen im Jahresbericht unzulässig sind. Auch die „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ (Bekanntmachung vom 19.04.2001, KWMBl I Seite 112, s. dazu auch Nr. 16.1.2) führten bisher unter Ziffer 4.4 Buchstabe d aus, dass die Herausgabe eines Jahresberichts für die Schüler und Erziehungsberechtigten der Schule nach Art. 85 Abs. 3

BayEUG zulässig ist, sofern nur die dort aufgeführten personenbezogenen Daten enthalten sind. Mit Einwilligung der jeweils Betroffenen bzw. bei minderjährigen Schülern eines Erziehungsberechtigten könnten zur Illustration des Jahresberichts Klassenfotos, Fotos einzelner Schüler oder Schülergruppen aufgenommen werden.

Auch das Einholen einer Einwilligung führt nach meiner Auffassung nach nicht zur Zulässigkeit des Einstellens der Wohnadresse in die Jahresberichte. Datenschutzrechtlich entscheidend ist, dass Art. 85 Abs. 3 BayEUG eine abschließende Regelung trifft und durch das Einholen der Einwilligung nicht erweitert werden kann. Der abschließende Charakter dieser Regelung ergibt sich unter anderem daraus, dass wegen der Möglichkeit der Weiterverbreitung der Jahresberichte über den eigentlichen Adressatenkreis der Schüler und Erziehungsberechtigten hinaus, die Jahresberichte bei der Angabe der Wohnadresse leicht für sachfremde - insbesondere kommerzielle - Zwecke verwendet werden können. Die Gefahr einer zweckwidrigen kommerziellen Verwendung besteht insbesondere bei Schülern der Abschlussklassen, da diese als Zielgruppe für Unternehmen, wie z. B. Banken und Versicherungen, besonders interessant sind. Diese Gefahr besteht beispielsweise bei dem Einstellen von Fotos in den Jahresbericht nicht, da hier nicht ohne weiteres ein Kontakt zu den Betroffenen hergestellt werden kann.

Das Bayerische Staatsministerium für Unterricht und Kultus teilt meine Auffassung nicht. Gleichwohl solle eine Veröffentlichung wegen der Gefahr missbräuchlicher Nutzung unterbleiben. Das Ministerium hat zwischenzeitlich mit Bekanntmachung vom 10.10.2002 (KWMBl I Seite 354) in den „Erläuternden Hinweisen für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ ausgeführt, dass die Aufnahme weiterer personenbezogener Daten von Schülern und Lehrern allenfalls mit deren Einwilligung zulässig sei, aber grundsätzlich (und insbesondere bei der Aufnahme der Wohnadressen) von der Einholung der Einwilligung abgesehen werden sollte.

Ich halte an meiner Auffassung fest, da die gesetzliche Lage für mich eindeutig ist. Ich begrüße es jedoch, dass immerhin von der Einholung der Einwilligung abgeraten wird.

16.1.6 Erstellung von Schülerfotos

Durch einige Eingaben habe ich von Foto-Aktionen an Schulen zur **Ausstellung von Schülerausweisen** erfahren. Eltern hatten sich in zahlreichen Fällen darüber beschwert, dass von ihren kleinen Kindern (1. bis 4. Klasse) ohne Wissen und Einverständnis der Eltern von einer privaten Firma Fotos für angebliche Schülerausweise gemacht wurden. Die Eltern waren über die Verwendung der Fotos und der Schülerdaten in Sorge. Meine Ermittlungen haben ergeben, dass die Firma von den Schulen mit der Anfertigung der Fotos für Schülerausweise beauftragt worden war.

Diese Fälle zeigen, dass den Schulen die Bestimmungen zur **Datenverarbeitung im Auftrag** nicht gegenwärtig waren. Insbesondere wurde nicht berücksichtigt, dass Schülerausweise erst ab der Jahrgangsstufe 5 erforderlich sind und eines Antrags bedürfen.

Wegen der aufgetretenen datenschutzrechtlichen Unzulänglichkeiten weise ich auf Folgendes hin:

Bei an den Schulen von Fotofirmen durchgeführten Foto-Aktionen zur Ausstellung von Schülerausweisen handelt es sich um Datenverarbeitungen im Auftrag gemäß Art. 6 BayDSG (s. dazu auch Nr. 4.6 der „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“, die auf meine Anregung hin aufgrund dieser Vorfälle ergänzt wurden (s. auch vorstehende Nr. 16.1.5) und Nr. 16.1.2 dieses TB). Die Schule ist als Auftraggeberin für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich (vgl. Art. 6 Abs. 1 Satz 1 BayDSG). Insbesondere ist gemäß Art. 6 Abs. 2 Satz 1 BayDSG der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Datenschutzmaßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei auch die technischen und organisatorischen Maßnahmen festzulegen sind, Art. 6 Abs. 2 Satz 2 BayDSG. Ferner hat sich die Schule soweit erforderlich von der Einhaltung dieser Maßnahmen beim Auftragnehmer zu überzeugen, Art. 6 Abs. 2 Satz 3 BayDSG. Ein Beispiel für einen **Mustervertrag zur Auftragsdatenverarbeitung** enthält meine Homepage (http://www.datenschutz-bayern.de) in der Rubrik „Technik“ unter „Orientierungshilfen/Mustervorlagen“.

Die datenschutzrechtliche Zulässigkeit der Weitergabe von Schülerdaten (Name, Geburtstag, Klasse) an die von der Schule mit der Erstellung von Fotos beauftragte Fotofirma richtet sich nach Art. 17 BayDSG, da es sich hierbei um Datennutzungen im Sinne des Art. 4 Abs. 7 und Abs. 10 Satz 2 i. V. m. Art. 6 Abs. 1 Satz 1 BayDSG handelt. Eine solche Nutzung ist u. a. nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der Schule liegenden Aufgaben erforderlich ist (vgl. Art. 17 Abs. 1 Nr. 1 BayDSG). Ausgehend von den Feststellungen des Bayerischen Staatsministeriums für Unterricht und Kultus in der Bekanntmachung vom 27.08.1996 (KWMBl I S. 339) ist diese Voraussetzung zumindest für Schüler von Grundschulen nicht erfüllt, da Schülerausweise erst ab der Jahrgangsstufe 5 auf Antrag vorgesehen sind.

Datenschutzrechtlich ist festzustellen, dass der Fotografiervorgang als Datenerhebung (Art. 4 Abs. 5 BayDSG) und die Datennutzung durch die Fotofirma in den Fällen, in denen die Voraussetzungen des Art. 85 Abs. 1 Satz 1 BayEUG bzw. des Art. 17 Abs. 1 BayDSG nicht vorliegen, nur mit freiwilliger, informierter und schriftlicher Einwilligung der Betroffenen bzw. des/der Erziehungsberechtigten zulässig sind. Dies betrifft alle Foto-Aktionen, die über das oben dargestellte Ausstellen von Schülerausweisen hinaus gehen.

16.2 Hochschulen

16.2.1 Hinweise zur Veröffentlichung von Mitarbeiterdaten im Internet für die bayerischen Hochschulen

Bereits in Nr. 12.3 meines 18. Tätigkeitsberichts habe ich mich grundsätzlich zur Zulässigkeit des Einstellens von Mitarbeiterdaten im Internet geäußert. Anlässlich einer Eingabe wurde ich auf das Problem der Veröffentlichung von Personaldaten der Mitarbeiter bayerischer Hochschulen durch das Einstellen von **Vorlesungsverzeichnissen** und **Stundenplänen** in das Internet hingewiesen. Vor diesem Hintergrund hat das Bayer. Staatsministerium für Wissenschaft, Forschung und Kunst **Hinweise zur Veröffentlichung von Mitarbeiterdaten im Internet** erarbeitet und diese mit mir abgestimmt; meine Empfehlungen wurden ausnahmslos berücksichtigt. Mit Schreiben vom 19.12.2001, Nr. X/10-23/11h(8)-10a/50 871, hat das Ministerium diese Hinweise an die Hochschulen mit der Bitte um Beachtung weitergegeben.

Danach kommt es bei der Beurteilung der Zulässigkeit der Veröffentlichung im Internet entscheidend darauf an, ob die Veröffentlichung der Daten zur Erfüllung der in der Zuständigkeit der Hochschule liegenden Aufgaben erforderlich ist. Bezüglich des Lehrangebots der Hochschule besteht ein berechtigtes Informationsinteresse Dritter, z. B. der Studierenden der jeweiligen Hochschule und potenzieller Studieninteressenten; die Hochschulen müssen über ihr Lehrangebot informieren. Aufgrund ihres Aufgabenbereichs müssen Lehrpersonen regelmäßig mit Dritten in Kontakt treten. Aus diesen Gründen kann die Erforderlichkeit für folgende Daten als gegeben angesehen werden:

1. Name, akademische Grade und Titel,
2. Dienstliche Anschrift,
3. Dienstliche Telefon- und Faxnummer,
4. Dienstliche E-Mail-Anschrift,
5. Aufgabenbereich, insbesondere Bezeichnung, Art, Zeit und Ort von Lehrveranstaltungen sowie Sprechzeiten.

Dabei sind folgende Einschränkungen zu machen:

Zu 3., 4.: Um Belästigungen oder eine Beeinträchtigungen der Arbeitssituation zu vermeiden, ist ohne die Einwilligung des Betroffenen nur die Veröffentlichung zentraler Telefon- bzw. Fax-Nummern oder E-Mail-Adressen zulässig (z. B. Telefonzentrale, Sekretariat, zentrale Posteinlaufstelle). Damit Außenstehende ohne Schwierigkeiten mit der betreffenden Lehrperson in Kontakt treten können, ist die Bereitstellung der genannten Daten ausreichend.

Zu 5.: Für Zwecke der Information über das an der Hochschule bestehende Angebot an Lehrveranstaltungen ist im Allgemeinen eine Recherche nach Themen bzw. Themengebieten, nicht jedoch eine gezielt auf eine Person bezogene Recherche notwendig. Da die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung auf das unabdingbar notwendige Maß zu beschränken ist, ist eine Aggregation der Vorlesungsdaten nach dem Namen der Lehrperson nur mit Einwilligung des Betroffenen zulässig. Insbesondere ist die Einwilligung des Betroffenen für entsprechende Suchfunktionen in Datenbank-gestützten Informationssystemen notwendig.

Die Veröffentlichung der Privatanschrift, der privaten Telefonnummer, der privaten E-Mail-Adresse, von Fotos und von anderen als den oben aufgeführten personenbezogenen Daten ist im Hinblick auf das Informationsinteresse Dritter nicht erforderlich. Sie ist daher nur mit der Einwilligung des Betroffenen zulässig.

Außerdem kann in Einzelfällen die schutzwürdige persönliche Situation des Betroffenen (z. B. einer gefährdeten Person) das Interesse der Hochschule am Einstellen personenbezogener Daten in das Internet überwiegen (Art. 15 Abs. 5 Satz 1 BayDSG).

Die Betroffenen müssen vor der Bereitstellung der Daten im Internet in geeigneter Form informiert werden; gegebenenfalls ist dies unverzüglich nachzuholen.

16.2.2 Nachweis krankheitsbedingter Prüfungsunfähigkeit bei Hochschulen

Aufgrund wiederholter Anfragen stellte ich fest, dass die datenschutzrechtlichen Maßgaben für ein Attest zum Nachweis der Prüfungsunfähigkeit häufig unbekannt sind. Die Frage des Nachweises krankheitsbedingter **Prüfungsunfähigkeit** wurde bereits in Abstimmung mit mir mit Schreiben vom 20.12.1993 Nr. X/4 - 6/185 592 vom damaligen Bayer. Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst mit folgendem Ergebnis behandelt:

„Das ärztliche Zeugnis muss die aktuellen krankheitsbedingten und zugleich prüfungsrelevanten körperlichen, geistigen und/oder seelischen Funktionsstörungen aus ärztlicher Sicht so konkret und nachvollziehbar beschreiben, dass der Prüfungsausschuss daraus schließen kann, ob am Prüfungstag tatsächlich Prüfungsunfähigkeit (= Rechtsbegriff!) bestanden hat. Das heißt, bei ambulanter oder anderer hausärztlicher Behandlung müssen aus dem ärztlichen Zeugnis die Hindernisse, an der Prüfung teilzunehmen, klar hervorgehen, z. B. notwendige Bettruhe, objektive Unfähigkeit, sich ohne erhebliche Beschwerden oder, ohne die Krankheitserscheinungen zu verschlimmern, zum Prüfungslokal zu begeben und/oder dort sich der Prüfung zu unterziehen, o.ä.. Das Zeugnis braucht **keine** medizinische Diagnose zu enthalten. Am Schluss des Zeugnisses soll der Arzt feststellen, ob er aus ärztlicher Sicht Prüfungsunfähigkeit annimmt.....“

Diese Anforderungen an den Inhalt eines ärztlichen Attests zum Nachweis der Prüfungsunfähigkeit sind Ausfluss der Rechtsprechung. Das Bundesverwaltungsgericht hat klargestellt, dass eine

ärztliche Bescheinigung, die sich darauf beschränkt, dem Prüfling Prüfungsunfähigkeit zu attestieren, für die Annahme der Prüfungsunfähigkeit nicht ausreichend ist. Es ist nicht Aufgabe eines Arztes, die Prüfungsunfähigkeit festzustellen. Prüfungsunfähigkeit ist ein Rechtsbegriff. Ob die Voraussetzungen hierfür gegeben sind, ist eine Rechtsfrage, die der Prüfungsausschuss und ggf. im Rahmen eines Rechtsstreits das Gericht anhand der vom ärztlichen Sachverständigen ihm zugänglich zu machenden Befunde in eigener Verantwortung zu beantworten hat.

17 Technischer und organisatorischer Bereich

17.1 Grundsatzthemen

17.1.1 Bayerisches Behördennetz

In meinem letzten Tätigkeitsbericht bin ich ausführlich auf die Entwicklung des Bayerischen Behördennetzes (BYBN) und des unter anderem damit verbundenen notwendigen Aufbaues einer Zertifizierungsstruktur zur sicheren Kommunikation eingegangen (vgl. 19. TB, Ziff. 17.1.2).

Im Berichtszeitraum wurde nun von einer Arbeitsgruppe unter Leitung des StMF in Zusammenarbeit mit einer Beratungsfirma der Entwurf einer Neukonzeption für das Bayerische Behördennetz, zukünftig BayKom genannt, erarbeitet. Neben der Berücksichtigung von wirtschaftlichen Aspekten ist eines der definierten Ziele der Neukonzeption auch die Gewährleistung höherer Sicherheitsanforderungen und –auflagen an den Betreiber. An den Beratungen der Arbeitsgruppe wurde teilweise auch meine Geschäftsstelle beteiligt, soweit es sich um datenschutzrelevante Teile des Konzeptes bzw. der daraus resultierenden Leistungsbeschreibung gehandelt hat. Ich habe mich für eine Präzisierung bezüglich einiger datenschutzrelevanter Formulierungen und Anforderungen eingesetzt. Das Bayerische Staatsministerium der Finanzen hat mir mitgeteilt, dass meine Anregungen bei der Überarbeitung der Leistungsbeschreibung berücksichtigt wurden.

Ein Zuschlag nach erfolgter Ausschreibung soll voraussichtlich Anfang 2003 erfolgen.

E-Mail

Auch in diesem Berichtszeitraum konnte der flächendeckende Einsatz einer starken Verschlüsselung unter Verwendung von S/MIME-Clients (z.B. Outlook 98, 2000 oder 2002) nicht umgesetzt werden. Mit ursächlich dafür ist die heterogene Softwareausstattung an den Arbeitsplätzen – von verwendeter Betriebssystemversion über verwendeten Mail-Client bis hin zum notwendigen Verzeichnisdienst.

Allerdings wurden inzwischen alle Behörden-Poststellen mit PGP ausgestattet, eine funktionierende Zertifizierungsstelle für PGP-Keys und ein Key-Server in Betrieb genommen - damit wäre ein sicherer E-Mail-Verkehr zwischen den angeschlossenen Poststellen und zwischen Bürger und Behörden jederzeit möglich – soweit der Bürger auf seinem heimischen PC ebenfalls PGP installiert hat. Leider hat die Firma NAI, der Lizenzinhaber von PGP, inzwischen angekündigt, das Produkt nicht mehr weiter zu entwickeln und den Support dafür eingestellt. Lediglich Fehlerbeseitigung wird noch für die Restlaufzeit der bestehenden Supportverträge Gewähr leistet. Nach derzeitiger Lage verbleibt allerdings das Nutzungsrecht der vom zentralen CERT beschafften und an die Poststellen verteilten PGP-Lizenzen auch nach Ablauf des Supportvertrages bei den derzeitigen Nutzern. Einer Weiterverwendung von PGP bis zur Installation einer endgültigen sicheren E-Mail-Lösung steht also nichts im Wege. Der im Herbst 2002 vollzogene Wechsel des Lizenzinhabers für PGP stellt eine Fortentwicklung des Produktes mit offengelegtem Quellcode und auch die Verfügbarkeit einer Freeware-Version für Privatanwender sicher.

Das vom Bundeswirtschaftsministerium favorisierte und auch geförderte Produkt OpenPGP wäre zwar grundsätzlich als durchaus empfehlenswerte Alternative anzusehen, allerdings ist meines Erachtens die von PGP gewohnte Benutzerfreundlichkeit, die besonders für den ungeübten Benutzer überaus wichtig ist, bei diesem Produkt noch nicht hinreichend gegeben. Außerdem hätte ein Produktwechsel für die Akzeptanz beim Nutzer sicher keine sehr förderliche Wirkung, da in den letzten Jahren im Bayerischen Behördennetz mehrfach verschiedene Produkte getestet wurden (vgl. 19. TB, Ziff. 17.1.2).

IuK-Gesetz

Mit in Kraft treten des IuK-Gesetzes (IuKG) vom 12.12.2001 (LTDrs 14/8267) – zur Ablösung des Gesetzes über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern (EDVG) vom 12.10.1970 (BayRS 200-3-I) - hat sich auch die Möglichkeit einer Neuorganisati-

on der bisher stark zergliederten Gremien für den Bereich der Sicherheit im ressortübergreifenden Kommunikationsverbund ergeben. Zu diesen Gremien habe ich mich auch im Abschnitt 17.1.2 meines 19. Tätigkeitsberichts geäussert.

Der Koordinierungsausschuss IuK (KoAIuK) hat in seiner Sitzung vom 12. Juni 2002 festgelegt, dass die übergreifende Verantwortung für die IuK-Sicherheit im staatlichen Bereich dem Staatsministerium des Innern obliegt und hierzu die Institution eines „Chief Information Security Officer“ (CISO) geschaffen wird. Zu dessen Unterstützung wird voraussichtlich beim Landesamt für Statistik und Datenverarbeitung ein „Computer Emergency und Response Team“ (CERT) eingerichtet und ein Sicherheitsteam aus den von den Ressorts bestellten Beauftragten für die IT-Sicherheit gebildet.

Diese Entscheidung könnte die von mir schon lange angemahnte Grundlage für eine kompetente, über Ressortgrenzen hinweg bindende Instanz für die Sicherheit der elektronischen Kommunikation innerhalb der Bayerischen Behörden bilden und so zu einer Steigerung der Sicherheit im Bayerischen Behördennetz beitragen.

Elektronische Signatur von Dokumenten in der öffentlichen Verwaltung

Der Bayerische Ministerrat hat in seiner Sitzung vom 9. Juli 2002 beschlossen, in der Staatsverwaltung flächendeckend bis spätestens zum Jahr 2005 die qualifizierte elektronische Signatur einzuführen, um so eine sichere elektronische Kommunikation zwischen Verwaltung und Bürger zu gewährleisten – so weit diese Art der elektronischen Signatur rechtlich erforderlich ist. In diesem Zusammenhang verweise ich auf den Entwurf eines Gesetzes zur Stärkung der elektronischen Verwaltungstätigkeit, der inzwischen kurz vor der Verabschiedung steht. Mit ihm sollen z.B. Verwaltungsverfahrensgesetz, Meldegesetz dahingehend geändert werden, dass auch die elektronische Kommunikation zwischen Bürger und Verwaltung als rechtswirksam zugelassen und zunehmend ausgebaut wird.

Zur elektronischen Kommunikation innerhalb der Verwaltung hat der Bayerische Ministerrat überdies beschlossen, dass die Behörden des Freistaats Bayern zügig und flächendeckend mit dem Verfahren des Landesamtes für Statistik und Datenverarbeitung für sichere E-Mail ausgestattet werden. Dieses Verfahren nutzt die fortgeschrittene Signatur und ein Verschlüsselungsverfahren.

Zusammenfassung

Meiner immer wieder gestellten Forderung nach einer vertraulichen, authentischen und nicht manipulierbaren Datenübertragung ist noch nicht vollständig Rechnung getragen (es fehlen u.a. flächendeckende sichere E-Mail und Leitungsverschlüsselung – SSL).

Allerdings ist der Verwaltung durch den Ministerratsbeschluss ein eindeutiger Zeitrahmen zur Umsetzung der geforderten Maßnahmen gesetzt worden. Im Zusammenhang mit den erwähnten Neuregelungen des IuK-Gesetzes hoffe ich, dass sich dies als ein entscheidender Schritt zur Erfüllung meiner langjährigen Forderungen erweist.

17.1.2 eGovernment

Unter dem Sammelbegriff „eGovernment“ sind drei verschiedene Anwendungsbereiche erkennbar:

- Verwaltung zu Bürger und umgekehrt (Government to Citizen – G2C)
- Verwaltung zu Wirtschaft und umgekehrt (Government to Business – G2B)
- Verwaltung zu Verwaltung und umgekehrt (Government to Government – G2G)

Beispiele für G2C in Bayern finden sich im Bereich der elektronischen Kommunikation im Media@KOMM-Projekt im Raum Nürnberg (vgl. 19. TB, Ziff. 17.3.2) sowie bei der elektronischen Steuererklärung ELSTER (vgl. 18. TB, Ziff. 19.3.12 und 19. TB, Ziff. 11.2) und in den in verschiedensten Behörden eingerichteten Bürgerbüros (vgl. 19. TB, Ziff. 8.5).

Als Beispiele für G2B in Bayern sei hier SOLUM-Star angeführt, auf das ich in den Abschnitten 7.6.9 und 18.2.4 meines 17. Tätigkeitsberichts bereits eingegangen bin, sowie das Projekt „Verdiensterhebung über das Internet“ (vgl. 19. TB, Ziff. 17.3.10).

Für den Bereich G2G ist vor allem das Bayerische Behördennetz anzuführen, auf das ich zuletzt in Abschnitt 17.1.2 meines 19. Tätigkeitsberichts sowie hier in Abschnitt 17.1.1 eingegangen bin.

Die Fragen nach Datenschutz und Datensicherheit spielen beim eGovernment eine entscheidende Rolle - auch für dessen Akzeptanz durch Bürger und Wirtschaft. So stellt z.B. die aus operativer Sicht sicherlich wünschenswerte Möglichkeit nach automatisierten Datenabgleichen mit Melderegistern und deren technische Machbarkeit noch keine Rechtsgrundlage für deren Zulässigkeit dar.

Hier sind in letzter Zeit erhebliche Anstrengungen vom Gesetzgeber unternommen worden, bestehende Rechtsnormen um die Aspekte der elektronischen Datenverarbeitung zu ergänzen. Als Beispiele seien hier nur die Novellierungen des Verwaltungsverfahrensgesetzes, des Melderechtsrahmengesetzes und der Abgabenordnung genannt. Solange diese Novellierungsarbeiten und deren ggfs. erforderliche Umsetzung in Landesrecht jedoch nicht abgeschlossen sind, muss die Realisierung und Inbetriebnahme solcher innovativer Vorhaben bis dahin aufgeschoben werden, zumal insbesondere die jeweiligen zu beachtenden technischen und organisatorischen Rahmenbedingungen zum jetzigen Zeitpunkt nicht absehbar sind.

Grundsätzlich ist bei allen Lösungen aus technisch-organisatorischer Sicht zum einen sicherzustellen, dass eine sichere und vertrauliche Kommunikation zwischen den jeweiligen Kommunikationspartnern gewährleistet wird – ungeachtet des verwendeten und zugrundeliegenden Kommunikationsnetzes. Die technischen Mittel hierzu stehen in Form von Kryptografieprodukten auf dem Markt zur Verfügung - es gilt, die geeigneten auszuwählen und auch einzusetzen.

Zum anderen ist von Seiten der öffentlichen Verwaltung auch sicherzustellen, dass mit Anbindung der eigenen Datenverarbeitungsanlagen und Verwaltungsnetzwerke an offene oder öffentliche Netzwerke, d.h. mit der Herbeiführung von deren Erreichbarkeit von außen, für diese Systeme und die darauf verarbeiteten Daten keine zusätzlichen Risiken entstehen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich bereits in ihrer Entschließung „Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ anlässlich der 60. Datenschutzkonferenz vom 12./13.Oktober 2000 hierzu geäußert (vgl. 19. TB, Anlage 26). Die in Abschnitt 8.5 meines 19. Tätigkeitsbericht angesprochene Broschüre „Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ ist unter http://www.datenschutz-bayern.de/technik/grundsatz/so_verw.pdf auf meiner Home-Page abrufbar.

Darüber hinaus sind die Datenschutzbeauftragten des Bundes und der Länder in einer Arbeitsgruppe „eGovernment“ unter der Leitung des Landesbeauftragten für den Datenschutz Niedersachsen derzeit damit befasst, eine entsprechende Broschüre mit weiteren praktischen Anregungen zu dem Thema zu erstellen. Mit deren Fertigstellung wird im Frühjahr 2003 zu rechnen sein. Auch diese Broschüre wird zum gegebenen Zeitpunkt über meine Home-Page www.datenschutz-bayern.de zum Abruf bereitgestellt werden.

17.1.3 Prüfkriterien für datenschutzfreundliche Produkte (Common Criteria)

Im Abschnitt 17.1.4 meines 19. Tätigkeitsberichtes, „Prüfkriterien für datenschutzfreundliche Produkte (Common Criteria)“, habe ich berichtet, dass der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe unter meiner Federführung gebildet hat, die zunächst ein Schutzprofil zu den Aspekten Verschlüsselung und Pseudonymisierung erstellen soll, um so bereits im Vorfeld von Produktentwicklungen wesentliche datenschutzrechtliche Anforderungen widergeben zu können.

Im Laufe der Entwicklungsarbeiten wurde deutlich, dass die Verwendungsbreite von Produkten auf Basis des zu entwickelnden Schutzprofils nicht nur den Bereich der Pseudonymisierung, sondern auch die verschlüsselte lokale Datenspeicherung und die sichere Datenübertragung über Netzwerke (z. B. im Gesundheitsbereich, der Statistik, der Forschung) umfassen könnte. Weitere Anwendungsmöglichkeiten derartiger Produkte wurden in den Bereichen Data-Warehouses, E-Commerce sowie bei Tele- und Mediendiensten erkannt und Mitte 2000 lag der erste Entwurf des Schutzprofils in den beschreibenden Teilen vor.

Für die Definition und Spezifikation der tiefergehenden Beschreibungen nach Common Criteria V2.1 – insbesondere für die so genannten „Funktionalen Sicherheitsanforderungen“ – wurde im September 2000 das BSI gebeten, die Fertigstellung und Fortentwicklung des Schutzprofils sowie dessen Evaluierung und formale Registrierung zu übernehmen.

Nach einigen verwaltungstechnischen Schwierigkeiten und einer entsprechenden Projektausschreibung beauftragte das BSI sodann im Sommer 2001 das Deutsche Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) mit der entsprechenden Schutzprofilfertigstellung.

Im September 2001 nahm die DFKI GmbH mit einem Kickoff-Workshop die Arbeit an dem nun „Benutzerbestimmbare Informationsflusssicherheit (BISS)“ genannten Projekt auf. An diesem nahmen neben dem BSI, den Vertretern des Bundesbeauftragten für den Datenschutz und meiner Dienststelle auch Vertreter mehrerer namhafter Unternehmen der Privatwirtschaft aus den Bereichen der Betriebssysteme, der Anwendungssoftware und der Sicherheitssysteme teil und wurden damit in den Entwicklungsprozess eingebunden.

Die weitere Projektarbeit stellte sich sodann als ausgesprochen komplex und arbeitsintensiv dar. Als Ergebnis sind jedoch nunmehr die folgenden, im Sommer 2002 evaluierten und registrierten Schutzprofile vorzuweisen:

- Benutzerbestimmbare Informationsflusskontrolle (MU) - als Mehrbenutzervariante
- Benutzerbestimmbare Informationsflusskontrolle (SU) - als Einbenutzervariante

Ihre wesentlichen Leistungsmerkmale sind:

- Transparenter Schutz der Informationsflüsse eines IT-Systems anhand definierbarer Regeln
- Bereitstellung von Mechanismen zur Sicherstellung von Vertraulichkeit, Integrität und/oder Authentizität durch elektronische Signatur, Verschlüsselung und elektronische Zertifikate
- Freie Kombinierbarkeit dieser Sicherheitsmechanismen für jeden einzelnen Informationsfluss in Abhängigkeit von seinem jeweiligen Schutzbedarf
- Freie Realisierbarkeit der erforderlichen kryptografischen Funktionen als Hardware, Firmware und/oder Software. Das zum Schutzprofil konforme Produkt muss keine eigene Krypto-Funktionalität aufweisen. Diese kann auch von einem anderen vertrauenswürdigen IT-Produkt (z.B. Smartcard) erbracht werden.
- Einschränkbarkeit der Verarbeitung von Informationen z.B. auf bestimmte Applikationen
- Geringer bis kein Anpassungsbedarf bei den bereits eingesetzten Applikationen
- Realisierbarkeit für unterschiedliche Umgebungen wie z.B. (Mehrbenutzer-) Betriebssysteme, Datenbanksysteme oder E-Mail-Clients und -Server
- Sinnvolle Ergänzung zu etablierten Sicherheitskonzepten wie etwa Zugriffsschutz, Übertragungsschutz, Firewalls und Virtual Private Networks
- Unterscheidbarkeit von Benutzern je nach verwendetem Schutzprofil

Die Schutzprofile können im Internet unter http://www.bsi.bund.de/cc/pplist/pplist.htm sowie http://dic.dfki.de eingesehen werden.

Datenschutzkonformität ist somit zu einem nachprüfbaren Qualitätsmerkmal für IT-Produkte geworden.

Es kommt nun darauf an, dass die Hersteller entsprechende Produkte entwickeln bzw. evtl. bereits existente Produkte entsprechend modifizieren und die Anwender von den Herstellern Produkte fordern, die diesen Schutzprofilen gerecht werden, d.h. entsprechend evaluiert sind.

17.1.4 Biometrische Verfahren

Die heute übliche Methode zur elektronischen Verifikation der Identität einer Person ist die Verwendung einer PIN oder eines Passwortes. Da mit zunehmender Anzahl der elektronischen Authentifizierungsverfahren auch die Anzahl der verschiedenen Passwörter zunimmt, wird es immer schwieriger, diese nicht zu vergessen. Eine Lösung für dieses Problem ist die biometrische Authentifizierung durch elektronische Systeme.

Biometrische Verfahren können zum einen für die Verifikation der Identität einer Person verwendet werden, beispielsweise in Zugangskontrollen, in denen nur die „echte“ Person als solche erkannt und zugelassen werden darf. Dabei werden biometrische Merkmale der Person mit vorgelegten (z.B. den auf einem Ausweisdokument gespeicherten digitalisierten biometrischen Merkmalen) Referenzdaten verglichen. Ein anderes Einsatzgebiet ist die Identifizierung einer Person aus einer Menge von (Referenz-)Personen heraus, durch Vergleich der von der Person präsentierten biometrischen Merkmale mit im DV-System (digitalisiert) gespeicherten biometrischen Merkmalen einer Vielzahl von Personen.

Die nach dem 11. September 2001 stattfindende Sicherheitsdiskussion hat ebenfalls die Biometrie als zusätzliches Hilfsmittel bei der Identifikation und Verifikation von Personen ins Rampenlicht gebracht. Es wird seitdem weltweit vermehrt versucht, kritische Bereiche wie z.B. Flughäfen mit biometrischen Systemen zu sichern.

Allgemein versucht man bei biometrischen Systemen, ein ähnliches Verfahren wie bei der Erkennung eines Menschen durch einen anderen Menschen mittels eines rechnergestützten Systems mit Sensoren zu implementieren. Der Rechner nimmt über einen oder mehrere Sensoren bestimmte biometrische Erkennungsmerkmale einer Person auf und vergleicht diese mit bereits gespeicherten Referenzmustern. Passen Sensordaten und Referenzdaten gut genug zusammen, so gilt die Person als authentifiziert bzw. identifiziert. Bei der Verifizierung muss ein Referenzmuster mit den aktuellen Sensordaten verglichen werden, bei der Identifikation müssen die Sensordaten mit allen gespeicherten Mustern verglichen werden.

Biometrische Merkmale haben im Vergleich zu herkömmlichen Sicherheitsmerkmalen den Nachteil, dass sie nicht widerrufbar sind. Ein Passwort kann man ändern und das alte verliert damit seine Gültigkeit. Sind Fingerabdrücke beispielsweise einmal mittels einer Kopie reproduzierbar, so kann niemand die eigenen Fingerabdrücke ändern, um die Fälschungen ungültig zu machen.

Die Tests von biometrischen Erkennungssystemen in letzter Zeit haben gezeigt, dass es noch viele Probleme bei der Zuverlässigkeit der Systeme gibt. Solange die Systeme leicht zu täuschen sind und Fehlerkennungsraten sehr hoch liegen, muss auf alle Fälle sichergestellt sein, dass kein System ausschließlich auf Biometrie beruht. Allen Personen muss es möglich sein, im Falle eines Irrtums diesen zu korrigieren, in dem sie sich mit herkömmlichen Mitteln authentifizieren.

Die Zuverlässigkeit eines biometrischen Systems hängt davon ab, wie hoch die Fehlerrate bei der Erkennung ist. Dabei unterscheidet man die Rate der irrtümlichen Erkennung (False Acceptance) und die der irrtümlichen Ablehnung (False Rejection). Bis zu einer bestimmten Abweichung zwischen Sensordaten und Referenzmuster gilt eine Person als erkannt. Diese maximal zugelassene Abweichung wird als Entscheidungsschwelle bezeichnet.

Ändert man die Entscheidungsschwelle in Richtung einer größeren erlaubten Abweichung, so werden mehr Personen akzeptiert. Die Ablehnungsrate sinkt zwar, aber es werden auch mehr Personen irrtümlich erkannt. Umgekehrtes gilt bei der Verschiebung in die andere Richtung. Die Rate der irrtümlich Abgewiesenen steigt. Je nach Anwendungsgebiet des biometrischen Systems sind die beiden Fehlerraten unterschiedlich kritisch. Ein System, das den Zugang zu einem geschützten Bereich ermöglichen soll, darf keinesfalls unberechtigten Personen Zutritt gewähren. Es ist allerdings weniger schlimm, wenn ein Zugangsberechtigter eventuell nicht zugelassen

wird. Wenn andererseits ein System eine gesuchte Person in einer Menschenmenge identifizieren soll, ist es aus operativen Gründen sicher besser, wenn es mehrere „Treffer“ anzeigt, unter denen sich die gesuchte Person befindet (false acceptance), als wenn es die eine gesuchte Person nicht bemerkt (false rejection). Beide Fehlerraten beeinflussen sich also und müssen für den jeweiligen Anwendungsfall optimiert werden.

Als biometrische Erkennungsmerkmale können unter anderem folgende verwendet werden:

- Fingerabdruck (Pappilarleistengebilde)
- Augeniris
- Gesicht
- Stimme
- Handgeometrie
- Unterschrift
- Bewegungsmuster

Zur Authentifizierung werden davon in herkömmlichen, nicht elektronischen Verfahren bereits das Bild des Gesichts und die Unterschrift auf Personalausweisen verwendet. Durch das Terrorismusbekämpfungsgesetz ist in § 4 Passgesetz und § 1 Personalausweisgesetz zusätzlich noch die Verwendung von biometrischen Merkmalen von Fingern, Händen oder Gesicht grundsätzlich erlaubt. Technische Einzelheiten insbesondere die Auswahl der biometrischen Merkmale bedürfen jedoch noch einer weiteren gesetzlichen Regelung.

Aus der Sicht des Datenschutzes muss sichergestellt werden, dass die biometrischen Referenzdaten in keiner zentralen Datei gespeichert werden, die auch für andere Aufgaben verwendet werden kann – dieses ist im o.a. Terrorismusgesetz auch so bestimmt.

Sollte es nötig sein, Daten außerhalb der Ausweisdokumente zu speichern, so dürfen keine überschiessenden Daten gespeichert werden, sondern nur die notwendigen Referenzdaten, sodass kein Rückschluss zum Beispiel auf gesundheitliche Eigenschaften getroffen werden kann.

Bei der bisherigen Form der Authentifizierung erfolgte diese grundsätzlich immer mit dem Wissen der Betroffenen. Einige biometrische Systeme können aber, zum Beispiel mit Kamerasensoren gekoppelt, Personen identifizieren, ohne dass diese dazu ihre Einwilligung erteilt haben. Bei

einer flächenmäßigen Erfassung könnten damit Bewegungsprofile erstellt werden, zum Beispiel wenn Kameras mit Gesichtserkennungssystemen gekoppelt würden. Da hier sensitive Daten ohne Wissen und Zustimmung der Betroffenen erhoben werden würden, lehne ich ein solches Szenario datenschutzrechtlich ab.

Die Datenschutzbeauftragten des Bundes und der Länder haben bei ihrer 63. Konferenz vom 07./08.03.2002 eine Entschließung zu „Biometrische Merkmale in Personalausweisen und Pässen“ gefasst, in der u.a. passive Systeme abgelehnt werden und darauf hingewiesen wird, dass eine zentrale oder dezentrale Speicherung der Merkmale nicht erlaubt ist. Des Weiteren sollten die verwendeten biometrischen Merkmale europaweit abgestimmt werden. Diese Entschließung ist als Anlage 19 beigefügt und auch auf meiner Home-Page unter http://www.datenschutz-bayern.de/dsbk-ent/63Biome.pdf abrufbar.

17.1.5 Auftragsdatenverarbeitung (Outsourcing von DV-Leistungen)

Ich wurde im Berichtszeitraum mehrfach von öffentlichen Stellen, die insbesondere aufgrund eines akuten Mangels an IT-Fachleuten in der öffentlichen Verwaltung den Betreuungsaufwand für ihre IT-Einrichtungen nicht mehr selbst erbringen können oder wollen, darauf angesprochen, unter welchen Voraussetzungen ein Outsourcing von DV-Leistungen möglich wäre. Einige dieser Behörden hatten bereits Kontakt mit externen Dienstleistern aufgenommen, die vermehrt DV-Dienstleistungen der unterschiedlichsten Art anbieten (z. B. Konzeption von DV-Systemen und Netzwerken, Entwicklung, Wartung und Pflege von Software, Wartung von Hardware, Administration einzelner Rechnersysteme beziehungsweise ganzer Netzwerke, Bereitstellung und Betrieb von Rechnersystemen oder von Rechenzentren, Beschaffung, Installation und Betreuung der Bürokommunikation).

Die Auslagerung der gesamten EDV wird anhand von Beispielen zweier Kommunen an anderer Stelle besprochen (siehe 17.3.3 – Outsourcing von Kommunaldaten).

Vor- und Nachteile

Vorteile eines Outsourcings können beispielsweise sein:

- Kosteneinsparung
- zusätzliche Einnahmen aus dem Verkauf der vorhandenen Hard- und Software
- Erhöhung der Planungssicherheit während der Dauer des Vertrages
- Beseitigung historisch gewachsener Probleme durch Neukonzeption
- Unabhängigkeit von Hard- und Softwareaufrüstungen bzw. –wechseln
- Unabhängigkeit von Personalqualifikationsproblemen und Personalengpässen
- hohe Flexibilität
- Konzentration auf die eigentlichen Kernaufgaben der öffentlichen Verwaltung
- Steigerung der Qualität der Datenverarbeitung
- effektiverer Datenschutz durch geschultes Personal und örtlichen Gegebenheiten

Allerdings muss sich genauso jede Behörde jeweils fragen, ob es nicht aus Datenschutzgründen besser wäre oder es notwendig ist, einzelne dieser Aufgaben durch eigene Kräfte zu erledigen. So ist beispielsweise bei medizinischen Daten der Schutz der Patientendaten gegen Beschlagnahme außerhalb der Krankenhäuser in der Regel nicht gewährleistet. Solange hier keine entsprechenden gesetzlichen Regelungen existieren, spreche ich mich gegen eine Auslagerung aus. Außerdem dürfen die Krankenhäuser nicht wesentliche Bereiche ihrer Datenverarbeitung in die Hände Dritter geben, damit sie sich nicht von diesen abhängig machen. Schließlich wäre bei einer solchen Auslagerung das Arztgeheimnis verletzt (ohne wirksame Patientenzustimmung). Gerade wegen der besonderen Sensibilität vieler Patientendaten müssen die Krankenhäuser ein gewisses Grund-Know-How im Umgang mit der Datenverarbeitung aufweisen können.

Ein weiterer Nachteil besteht darin, dass bei einer Auftragsdatenverarbeitung die Kontrolle der Einhaltung des Datenschutzes und der Datensicherheit nur im eingeschränkten Maße möglich ist.

Somit kann in manchen Fällen sehr schnell der Zustand erreicht werden, dass die Erreichung der mit dem Outsourcing angestrebten Ziele (Einsparung von Ressourcen) aufgrund der zu ergreifenden Datenschutz- und Datensicherungsmaßnahmen in Frage gestellt oder gar verfehlt wird. Auch eine Wirtschaftlichkeitsbetrachtung der Outsourcingmaßnahme unter Berücksichtigung des Aufwandes für die erforderlichen Sicherheitsmaßnahmen ist hier dringend geboten.

Zu bedenken ist auch, dass Outsourcing eine mittelfristig kaum widerrufbare Entscheidung ist, da es nach Aufgabe des eignen IT-Know-hows schwierig bis fast unmöglich wird, den Schritt rückgängig zu machen.

Rechtsvorschriften

Die folgenden Ausführungen beziehen sich insbesondere auf Art. 6 BayDSG (Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag). Allerdings ist zu berücksichtigen, dass bereichsspezifische Vorschriften dem Bayerischen Datenschutzgesetz vorgehen und zum Teil eine Auftragsdatenverarbeitung aus Geheimhaltungspflichten verbieten. Bereichsspezifische Vorschriften sind beispielsweise:

- Art. 36 des Bayerischen Meldegesetzes (MeldeG)
- Verletzung von Privatgeheimnissen (Berufsgeheimnissen) gemäß § 203 Abs. 1 StGB (z. B. für Ärzte)
- § 30 Abgabenordnung (Steuergeheimnis)
- § 80 SGBX (Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag)
- Art. 27 Abs. 4 – 6 Bayerisches Krankenhausgesetz (Verarbeitung von Patientendaten im Auftrag)

Verantwortliche Stelle

Wenn eine Behörde personenbezogene Daten durch eine andere Stelle erheben, verarbeiten oder nutzen lässt, so handelt es sich dabei gemäß Art. 6 BayDSG um eine Datenverarbeitung im Auftrag. Datenschutzrechtlich wird der externe Dienstleister in seiner Eigenschaft als Auftragnehmer so behandelt, als sei er eine interne Abteilung des Auftraggebers. Bei der Auftragsdatenverarbeitung wird lediglich eine „Hilfsfunktion“ der eigentlichen Aufgabe ausgelagert, nicht jedoch die Aufgabe selbst. Es findet somit keine Datenübermittlung im Sinne der Art. 18 und 19 BayDSG statt. Der Auftragnehmer erhält keine Entscheidungsbefugnis bezüglich der Daten. Deswegen bleibt der Auftraggeber gemäß Art. 6 Abs. 1 BayDSG für die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Dies betrifft insbesondere die Vorschriften für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die Wahrung der Rechte des Betroffenen sowie die Einhaltung der nach Art. 7 BayDSG erforderlichen Datensicherheitsmaßnahmen.

Der Auftragnehmer wird weder „Herr der Daten“ noch speichernde Stelle. Er darf die erhaltenen Daten nicht zu eigenständigen Zwecken nutzen und ist dem Auftraggeber gegenüber zur Einhaltung des Datenschutzes und der Datensicherheit verpflichtet.

Auswahlkriterien

Gemäß Art. 6 Abs. 2 Satz 1 BayDSG sind Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Wichtiges Auswahlkonzept ist somit das Datensicherheitskonzept des Auftragnehmers. Die Umsetzung dieses Konzeptes sollte durch den Datenschutzbeauftragten des Auftraggebers vor Ort in Augenschein genommen werden (siehe Art. 6 Abs. 2 Satz 3 BayDSG).

Gemäß Nr. 1 der Vollzugsbekanntmachung zum Bayerischen Datenschutzgesetz gelten das Landesamt für Statistik und Datenverarbeitung und die Anstalt für kommunale Datenverarbeitung (AKDB) als sorgfältig ausgewählte Auftragnehmer im Sinne des Art. 6 Abs. 2 Satz 1 BayDSG. Somit bleibt einem Auftragnehmer eine Prüfung der Eignung der von diesen Stellen getroffenen technischen und organisatorischen Maßnahmen erspart.

Vertragsgestaltung

Der Auftrag ist schriftlich zu erteilen (Art. 6 Abs. 2 Satz 2 BayDSG), wobei detailliert festzulegen sind,

- die Beschreibung des Vertragsgegenstandes,
- die Art und der Umfang der Datenerhebung, -verarbeitung oder -nutzung,
- das Verbot der Benutzung der Daten zu anderen Zwecken bzw. deren unerlaubten Weitergabe,
- Auftrags- und Realisierungszeitraum,
- Vertragsdauer,
- Modalitäten einer vorzeitigen Kündigung,
- Eigentumsrechte an Hard- und Software,
- System- und Benutzerdokumentation,
- Aufbewahrungspflichten,
- Gewährleistungsansprüche,
- Haftung,

- die vom Auftragnehmer einzuhaltenden technischen und organisatorischen Maßnahmen (inklusive deren Fortschreibung) und
- ob und unter welchen Voraussetzungen es zulässig ist, Subunternehmer heranzuziehen.

Dabei ist insbesondere zu regeln:

- Beschreibung der organisatorischen, räumlichen und personellen Maßnahmen zur Gewährleistung der Datensicherheit
- Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung des Datengeheimnisses gemäß § 5 BDSG
- Versendungs- und Aufbewahrungsrichtlinien für Datenträger
- Zeitpunkt und Art der Löschung bzw. Vernichtung von Datenträgern
- Kontroll- und Weisungsrecht des Auftraggebers (auch gegenüber etwaigen Subunternehmern).

Auch eventuelle Schadensersatzforderungen sollten im Vertrag aufgenommen werden.

Überprüfung des Einhaltens der Regelungen

Der Auftraggeber muss – wie erwähnt – soweit erforderlich die Einhaltung der getroffenen Regelungen überprüfen (Art. 6 Abs. 2 Satz 3 BayDSG), damit gewährleistet ist, dass die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten durch den Auftragnehmer nur entsprechend den Weisungen des Auftraggebers erfolgt. Ein Auftraggeber sollte sich nicht mit der bloßen Erklärung des Auftragnehmers zufrieden geben, dass dieser die Vorschriften der Datenschutzgesetze beachten werde. Zur Ermöglichung der Überprüfung bedarf es der Einräumung eines Betretungsrechtes für die Betriebs- oder Geschäftsräume des Auftragnehmers.

Wesentliche Änderungen des Datensicherheitskonzeptes des Auftragnehmers müssen dem Auftraggeber unverzüglich mitgeteilt werden. Dies gilt auch für Störungen, Mängel oder andere Unregelmäßigkeiten im Verarbeitungsablauf.

Weitere Pflichten des Auftragnehmers

Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen (Art. 6 Abs. 3 Satz 2 BayDSG). Die Speicherung von personenbezogenen Daten ist nur während der Durchführung des Auftrages gestattet. Eine Weitergabe von per-

sonenbezogenen Daten an Dritte ist nur im Rahmen des Vertrages zulässig. Auch eine Verarbeitung der personenbezogenen Daten für andere Zwecke ist unzulässig.

Ist ein Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Bayerische Datenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen (Art. 6 Abs. 3 Satz 3 BayDSG).

Abgrenzung zur Funktionsübertragung

Um keine Form der Auftragsdatenverarbeitung im Sinne des Bayerischen Datenschutzgesetzes handelt es sich bei der so genannten Funktionsübertragung. Bei einer Funktionsübertragung wird nicht nur eine genau definierte Dienstleistung, sondern die Erfüllung einer bestimmten Aufgabe (z.B. die Lohn- und Gehaltsabrechnung) oder zumindest wesentlicher Teile einer Aufgabe übertragen.

Bei einer Funktionsübertragung findet im Gegensatz zu einer Auftragsdatenverarbeitung eine Datenübermittlung im rechtlichen Sinne statt. Der Auftragnehmer wird damit zur speichernden Stelle und erhält die Nutzungsrechte an den Daten und ist für deren Zulässigkeit und Richtigkeit verantwortlich. Außerdem ist bei einer Funktionsübertragung der Auftragnehmer für die Gewährleistung des Datenschutzes und der Datensicherheit im Rahmen der übertragenen Aufgabe verantwortlich.

17.1.6 Novelliertes Bayerisches Datenschutzgesetz (BayDSG)

Mit dem Gesetz zur Änderung des Bayerischen Datenschutzgesetzes vom 25.Oktober 2000 sind zahlreiche Bestimmungen des Bayerischen Datenschutzgesetzes (BayDSG) in der überwiegenden Anzahl zum 01.12.2000, teilweise auch zum 01.03.2001, geändert worden. Ursächlich hierfür war überwiegend die Notwendigkeit zur Umsetzung der Vorgaben der EG-Datenschutzrichtlinie 95/46/EG vom 24.10.1995 (Abl. EG Nr. L 281/31). Ich verweise auf meine Darstellung im 19. TB unter Nr. 2.2.2.

Aus technisch-organisatorischer Sicht sind im Rahmen der gemachten Änderungen insbesondere von Bedeutung:

Prüfung und Wartung automatisierter Verfahren und Datenverarbeitungsanlagen

Diese Regelung über die Prüfung und Wartung automatisierter Verfahren und Datenverarbeitungsanlagen wurde mit Art. 6 Abs. 4 BayDSG neu eingeführt.

Datenschutzrechtliche Freigabe

- Delegation zur datenschutzrechtlichen Freigabe selbstentwickelter Verfahren auf die das Verfahren einsetzende öffentliche Stelle (Art. 26 Abs. 1 Satz 1 BayDSG)
  Dadurch ist es möglich, vor Ort entwickelte Verfahren auch unmittelbar dort datenschutzrechtlich freizugeben. Beibehalten wurden die bisherigen Regelungen bzgl. Verfahren, die von der Anstalt für Kommunale Datenverarbeitung oder vom fachlich zuständigen Staatsministerium freigegeben und von der das Verfahren einsetzenden öffentlichen Stelle unverändert übernommen werden.

- Delegation der Freigabebefugnis auf den behördlichen Datenschutzbeauftragten (Art. 26 Abs. 3 Satz 2 BayDSG)
  Mit dieser Änderung wird die Befugnis zur datenschutzrechtlichen Freigabe von Verfahren für den Regelfall auf den behördlichen Datenschutzbeauftragten delegiert.
  Hat der behördliche Datenschutzbeauftragte Bedenken, dass das Verfahren den Datenschutzvorschriften nicht genügt, und werden diesen nicht Rechnung getragen, so legt er die Entscheidung über die Freigabe der Person vor, der er nach Art. 25 Abs. 3 Satz 1 BayDSG unterstellt ist. Diese entscheidet dann, ob sie die Freigabe selbst erteilt oder verweigert.
  Ist die Verarbeitung besonders sensibler Daten nach Art. 15 Abs. 7 BayDSG beabsichtigt, so hat der behördliche Datenschutzbeauftragte bei Bedenken vor einer Vorlage an die Person, der er nach Art. 25 Abs. 3 Satz 1 BayDSG unterstellt ist, zunächst meine Stellungnahme einzuholen (Art. 26 Abs. 3 Satz 3 BayDSG).

- Erweiterter Umfang der datenschutzrechtlichen Freigabe (Art. 26 Abs. 2 BayDSG)
  Die bisherigen sieben Nrn. wurden inhaltlich unverändert beibehalten. Neu aufgenommen wurden die Nrn. 8 und 9, d.h. Angaben zu Auftragnehmern bei Auftragsdatenverarbeitung gem. Art. 6 Abs. 1 mit 3 BayDSG und Angaben zu den Empfängern von Datenübermittlungen, in deren Länder die EG-Datenschutzrichtlinie nicht gilt.
  Eine erneute datenschutzrechtliche Freigabe von bereits freigegebenen Verfahren ist auf-

grund dieser Gesetzesänderungen nicht erforderlich – es sei denn, am betreffenden Verfahren werden wesentliche Änderungen vorgenommen (vgl. Art. 26 Abs. 1 Satz 3 BayDSG); diese neue Freigabe ist dann gemäß den nunmehr geltenden Vorschriften vorzunehmen. Ein Muster-Formblatt für die Verfahrensbeschreibung nach der neuen Fassung des Art. 26 Abs. 2 BayDSG steht auf meiner Home-Page unter http://www.datenschutz-bayern.de/inhalte/technik.htm zur Verfügung.

Verfahrensverzeichnis und Anlagenverzeichnis

- Konkretisierte Verpflichtung zur Führung des Verfahrensverzeichnisses durch den behördlichen Datenschutzbeauftragten (Art. 27 Abs. 1 BayDSG)
  Die bisherige Bestimmung, dass öffentliche Stellen ein Verzeichnis der bei ihnen eingesetzten freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, d.h. ein Verfahrensverzeichnis zu führen haben, wurde dahin präzisiert, dass dieses Verfahrensverzeichnis durch den behördlichen Datenschutzbeauftragten zu führen ist.
  In dem Verzeichnis sind nach Art. 27 Abs. 2 BayDSG für jedes Verfahren die Angaben, die auch für die datenschutzrechtliche Freigabe nach Art. 26 Abs. 2 BayDSG erforderlich sind, festzuhalten. Für die Praxis bedeutet dies, dass z.B. die geordnete Sammlung ausgedruckter datenschutzrechtlicher Freigaben das Verfahrensverzeichnis bildet.

- Streichen der Verpflichtung, ein Anlagenverzeichnis zu führen (Art. 27 Abs. 1 BayDSG)
  Die bisherige Verpflichtung, neben dem Verfahrensverzeichnis ein Anlagenverzeichnis zu führen, wurde gestrichen und durch die Aufnahme der Verpflichtung, der Verfahrensbeschreibung eine allgemeine Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen nach Art. 7 und 8 BayDSG beizugeben (Art. 26 Abs. 3 Satz 1 BayDSG) ersetzt.

- Neueinführung, dass das Verfahrensverzeichnis von jedem kostenfrei eingesehen werden kann (Art. 27 Abs. 3 Satz 1 BayDSG).
  Dieses Recht zur Einsichtnahme bezieht sich nur auf die nach Art. 26 Abs. 2 BayDSG erforderlichen Angaben der datenschutzrechtlichen Freigabe; die nach Art. 26 Abs. 3 Satz 1 BayDSG der Verfahrensbeschreibung beizugebenden Angaben zu den Datenverarbeitungsanlagen und zu den technischen und organisatorischen Maßnahmen sind davon nicht

umfasst. Es empfiehlt sich daher - auch aus Sicherheitsgründen - , die technischen Beschreibungen von dem Verfahrensverzeichnis getrennt zu führen, um so bei einer Einsichtnahme in das Verfahrensverzeichnis nicht unnötigerweise auch die technischen Beschreibungen offen zu legen.

- Wegfall der Verpflichtung zur Bestellung behördlicher Datenschutzbeauftragter, der datenschutzrechtlichen Freigabe und der Aufnahme in ein Verfahrensverzeichnis bei denjenigen öffentlichen Stellen, bei denen durch Rechtsverordnung abschließend der Umfang der erhobenen, verarbeiteten oder genutzten Daten festgelegt wird (Art. 28 Abs. 2 BayDSG).

Nicht umgesetzt wurden leider weitere Änderungsvorschläge aus dem technisch-organisatorischen Bereich z.B. zur Einführung von Regelungen über Videoüberwachung und Chipkarten sowie zur „Modernisierung“ der „10 Gebote“ der technischen und organisatorischen Maßnahmen (vgl. Art. 7 Abs. 2 BayDSG), so dass hier nunmehr Unterschiede zum diesbezüglich novellierten Bundesdatenschutzgesetz bestehen. Diese Änderungsvorschläge bleiben einer zweiten Novellierungsstufe des BayDSG vorbehalten.

17.1.7 Der Internetauftritt

Immer mehr Stellen der öffentlichen Verwaltung erkennen das Internet als ein weiteres Medium zur Informations-Präsentation und zur eigenen Darstellung dem Bürger gegenüber. Die Veröffentlichung von Information und das Bereitstellen von Angeboten z.B. in Form von Formularen u.ä. ist als Teledienst im Sinne des § 2 Abs. 2 Teledienstegesetz (TDG) zu sehen. Somit sind sowohl das Teledienstegesetz als auch das Teledienstedatenschutzgesetz (TDDSG) auf Internetauftritte/Home-Pages anzuwenden.

Diese beiden Gesetze, gefasst als Art. 1 und 2 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz - IuKDG) vom 22.07.1997 (BGBl I, S. 1870), wurden mit dem Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG) vom 14.12.2001 (BGBl I, Nr. 70, S. 3721) novelliert.

Beide Gesetze legen dem Teledienstеanbieter, d.h. dem Betreiber der Home-Page, gewisse Informationspflichten auf. So verlangt § 6 TDG die leicht erkennbare, unmittelbar erreichbare und ständig verfügbare Bereitstellung von Informationen zum Teledienstеanbieter selbst. Diese geforderten Angaben können verglichen werden mit dem aus der gedruckten Presse bekannten Impressum und werden häufig auch als Anbieterkennzeichnung bezeichnet.

§ 4 Abs. 1 TDDSG verlangt, dass der Teledienstеanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten usw. zu unterrichten hat. Zum Inhalt dieser Vorabunterrichtung verweise ich auf Abschnitt 17.4 meines 19. Tätigkeitsberichtes und auf die in meiner Home-Page bereitgestellte Orientierungshilfe „Online-Datenschutz-Prinzipien (ODSP)“ (http://www.datenschutz-bayern.de/technik/orient/priv-pol.htm).

Hinsichtlich der Realisierungsmöglichkeiten für diese Unterrichtungspflichten verweise ich auf die o.g. Orientierungshilfe sowie auf die Orientierungshilfe „Tele- und Mediendienste“ meines Hamburger Kollegen (http://fhh.hamburg.de/coremedia/generator/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/veroeffentlichungen/informationsmaterialien/internet/orientierungshilfe-tele-und-mediendienste.html).

Besonders aufmerksam machen möchte ich insbesondere auf § 4 Abs. 4 Ziffer 3 TDDSG, wodurch der Teledienstеanbieter zwingend verpflichtet wird, kryptografische Mechanismen zur Wahrung der Vertraulichkeit, d.h. Verschlüsselungssysteme, anzubieten.

Im Berichtszeitraum habe ich die Internetauftritte verschiedenster Stellen der öffentlichen Verwaltung in Bayern besucht und auf die Aspekte des neu gefassten Teledienstegesetzes und Teledienstedatenschutzgesetzes hin überprüft. Dabei musste ich zum Teil erhebliche Defizite in der Umsetzung der Forderungen dieser beiden Gesetze feststellen. Ich weise darauf hin, dass Verstöße gegen diese gesetzlich geforderten Informationspflichten mit der Novellierung der Gesetze auch als Ordnungswidrigkeit zu betrachten sind, die mit einer Geldbuße bis zu € 50.000.-- geahndet werden können.

Es wird daher allen Anbietern von Internetauftritten dringend empfohlen, Ihre eigenen Internetauftritte hinsichtlich der Konformität zu den Forderungen des Teledienstegesetzes und des Teledienstedatenschutzgesetzes zu überprüfen und ggf. zu überarbeiten.

17.1.8 Anforderungen an Antivirenprogramme

Der Schutz von IT-Netzen gegen einen Virenbefall wird immer schwieriger. Immer neue Wege der Datenübertragung schaffen immer wieder neue Gefahren. Jahr für Jahr steigt die Anzahl neuer Viren und neuer Virenarten. Waren es früher „nur“ Datei- und Systemviren, gegen die sich ein Anwender schützen musste, so entstanden nach und nach weitere Arten von Schadenssoftware (Malware), wie z. B. Hybride Viren, Trojanische Pferde, Würmer, Makroviren, Script-Viren, Hostile Applets und Hoax-Viren. Auf diese Virenarten und die Möglichkeiten ihrer Bekämpfung bin ich in meinen früheren Tätigkeitsberichten (z. B. Nr. 18.1.7 – Makroviren im 17. TB, Nr. 19.3.8 Hoax-Viren und Hostile Applets im 18. TB oder Nr. 17.1.5 – Viren im Internet im 19. TB) bereits eingegangen.

War es früher ausreichend, Arbeitsplatzrechner ohne Disketten- und ohne CD-ROM-Laufwerk auszustatten, um den Import von Viren abzuwehren, steigt das Risiko eines Virenbefalls durch die Einrichtung von Intranets – insbesondere bei einem Anschluss an das Internet. So können Viren durch den E-Mail-Verkehr, beim Websurfen oder durch das Herunterladen von Dateien eingeschleust werden.

Die zuverlässigste Methode, um einen Computervirenbefall frühzeitig erkennen und beseitigen zu können, stellen Virenentdeckungsprogramme (so genannte Scanner) dar, mit denen Arbeitsspeicher und Datenträger regelmäßig auf Virenverseuchung untersucht werden können. Allerdings bietet auch diese Software keinen hundertprozentigen Schutz gegenüber einer Vireninfektion, da sie grundsätzlich nur die Viren suchen und bekämpfen kann, die ihr bereits bekannt sind. Das bedeutet, dass ein neuer Virus zunächst einmal einen Rechner befallen haben muss, damit er erkannt, in einer speziellen Datenbank beim Antivirensoftwarehersteller erfasst, isoliert und bekämpft werden kann. Also werden auch gute Virenscanner immer der Entwicklung zeitlich hinterherhinken. Sie bieten nach allgemeinen Schätzungen im Moment ihres Erscheinens bzw. Updates lediglich eine Sicherheit, bis zu 85 Prozent aller Viren erkennen zu können. Umso mehr

sollte jede öffentliche Stelle darauf achten, dass nur Scanner von Anbietern erworben werden, die einen regelmäßigen (möglichst täglichen) Update-Service gewährleisten.

Virenscanner sollten nicht nur das Eindringen von Viren soweit wie möglich verhindern oder zumindest erschweren, sondern auch die Ausbreitung bereits eingedrungener Viren unterbinden. Dazu suchen sie nach bereits bekannten Hex-Pattern, durch die sich ein Virus erkennen lässt. Das können bestimmte Befehlsfolgen oder Texte im Virenprogramm sein. Einige Antivirenprogramme überprüfen zusätzlich den Anfang und das Ende aller ausführbaren Dateien auf virentypisches Verhalten (heuristisches Verfahren). Diese Methode kann allerdings auch zu Fehlalarmen führen. Außerdem sind heuristische Scanner nicht in der Lage, Viren zu entfernen.

An dieser Stelle soll auch nicht verschwiegen werden, dass eine Beseitigung von Viren in einem ausführbaren Programm unter Umständen dazu führen kann, dass dieses Programm nach der Säuberung nicht mehr ablauffähig ist, da ein wichtiger Teil des Programmes bei der Desinfektion mitbeseitigt wurde. In einem solchen Falle ist es häufig besser, gleich das ganze Programm zu entfernen und durch die Originalfassung zu ersetzen.

Gute Antivirenprogramme sollten über folgende Bestandteile verfügen:

- Virensuchprogramm (Scanner) incl. heuristischem Suchen
- (Mit Hilfe von Virensuchprogrammen können Software und Datenträger schon vor dem Einsatz überprüft werden. Man kann damit eine Infektion mit bekannten Viren weitestgehend vermeiden. Mit vielen Scannern können durch die Betriebsart „heuristisches Suchen“ neue, bisher noch nicht bekannte Viren aufgespürt werden.)
- Prüfsummenverfahren (Integrity Checker)
- (Prüfsummenverfahren dienen der Überwachung der Unversehrtheit eines Programms. Sie errechnen für jede ausführbare Datei eine Prüfsumme aus einer Reihe von dateispezifischen Informationen (z. B. Erstellungsdatum, Dateigröße, Datum und Zeit der letzten Aktualisierung, Adresse der Datei auf dem Speichermedium) und speichern diese in einer eigenen Datenbank. Bei jedem Aufruf einer ausführbaren Datei werden deren Prüfsumme mit der in der Datenbank hinterlegten Prüfsumme verglichen. Programmänderungen, die eine Veränderung der Prüfsumme zur Folge haben, werden damit sofort erkannt.)
- Speicherresidente Wächterprogramme (Behavior Blocker)
  (Diese Programme überwachen alle Programmaktivitäten (einschließlich der Ausführung

von Makros) und melden ein verdächtiges „Benehmen“ – z. B. Schreibzugriffsversuche auf Systembereiche.).

Bei der Auswahl eines Antivirenprogramms sollte u. a. folgende Anforderungen an die Funktionalität, die Handhabung und die Sicherheit gestellt werden:

- Erkennen aller verbreiteten (in the wild = in freier Wildbahn) Viren
- einstellbarer Prüfablauf (On Demand = Starten von zeitgesteuerten Suchvorgängen (Scheduled-Scan) bzw. auf Benutzeranforderung und On Access = permanente Überwachung aller Dateizugriffe)
- umfangreiche Möglichkeiten der Virenbehandlung von infizierten Dateien (Löschen, Säubern, Umbenennen, Isolieren)
- Benutzer- bzw. Administratorbenachrichtigung bei Verdacht eines Virenbefalles
- Netzwerkunterstützung
- zentrale Administration
- aussagekräftige Protokollierung
- Ablaufsicherheit
- geringe Performance-Belastung
- Notfallhilfe (Erstellung einer Boot-Diskette etc.)
- Untersuchung von komprimierten Dateien
- Online-Dokumentation
- regelmäßiger Online-Update-Service
- automatischer Update der Clients per Log-in-Skript.

Bei einem Internet-Anschluss müssen spezielle Virenscanner zum Einsatz gelangen, die auch Script Viren und Hostile Applets aufspüren können und bei einem Befund den Zugriff dieser Programme auf den Rechner unterbinden sowie das Applet löschen. Unsichere Seiten, von denen die feindlichen Programme kamen, dürfen kein zweites Mal angesteuert werden können.

Mit Hilfe von Filtertechniken (Content-Filtering) sollte es möglich sein, E-Mails mit speziellen Dateianhängen (z. B. vbs = Visual Basic Script) zu blockieren.

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 (Gateway-Rechner) ist daher unverzichtbar. Auch ein laufendes Scannen der Arbeitsplatzrechner wird angeraten, insbesondere wenn diese PC mit Disketten- und/oder CD-ROM-Laufwerken ausgestattet sind.

Bereits am 01.08.1991 gab das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstmals „Forderungen an Viren-Suchprogramme“ heraus. Im Rahmen einer Arbeitsgruppe zwischen den für ITSEC zuständigen Behörden von Großbritannien und Deutschland entstand eine untereinander abgestimmte Fassung einer „Funktionalitätsklasse für Viren-Suchprogramme“. Diese Informationen können der BSI-Broschüre „Informationen zu Computer-Viren“ entnommen werden (im Internet abrufbar unter: http://www.bsi.de/av/virbro/anhang/anhang_c.htm).

17.1.9 Fernwartung und Einsatz von Remote Management (Control) Programmen (Fernbedienung)

Fernwartung

In der modernen Verwaltung wird heute eine Vielzahl von speziellen Rechnern und Verfahren eingesetzt, deren alleinige Wartung durch das eigene Personal wegen der dafür benötigten Spezialkenntnisse vielfach nicht mehr möglich ist, so dass bei Störungen sowie bei in der Hard- oder Software auftretenden Fehlern aufgrund der Abhängigkeit von einer funktionierenden IT-Verarbeitung oft der Hersteller eingeschaltet werden muss. Das geschieht zum Teil vor Ort, meist jedoch im Rahmen des Teleservice, also in Form einer Ferndiagnose und -wartung (unter Umständen auch durch den eigenen Systemverwalter von zu Hause aus – siehe unter Remote Management Programme). Die Vorteile einer Fernwartung sind insbesondere die schnellere Hilfe, geringere Kosten (auch wenn sicherlich der Aufbau einer Fernwartungszentrale ebenfalls mit Kosten verbunden ist) und die Verfügbarkeit von Spezialisten. Es besteht bei einer Fernwartung aber immer die Gefahr, dass sensible Informationen bewusst oder unbewusst an Unberechtigte offenbart werden.

Bei einer reinen Hardwarewartung wird in der Regel nur auf bestimmte Statusinformationen in eigens dafür eingerichteten Diagnosedateien zugegriffen, die keine personenbezogenen Daten enthalten. Bei vielen DV-Systemen kann aber die Fehlerdiagnose und -behebung mit einer Offenbarung geschützter personenbezogener Daten verbunden sein. Deshalb ist eine Fernwartung datenschutzrechtlich besonders problematisch. Bei einer Wartung vor Ort sind die Kontroll- und

Eingriffsmöglichkeiten des eigenen Personals im Regelfall größer. Es ist dann eher erkennbar und prüfbar, welche konkreten Personen in Erscheinung treten und ein unberechtigtes „Entfernen“, Verändern, Lesen oder Übertragen von Daten ist durch die Kontrolle erschwert.

Bei Einsatz einer Fernwartung ist daher insbesondere auf die Einhaltung folgender Regeln zu achten:

- Der Auftraggeber definiert Art und Umfang der Fernwartung sowie die Abgrenzung der Kompetenzen und Pflichten zwischen Wartungs- und Kundenpersonal im Wartungsvertrag. Für Zuwiderhandlungen sind empfindliche Vertragsstrafen vorzusehen.
- Das Wartungspersonal muss auf das Datengeheimnis verpflichtet sein.
- Eine Weitergabe der im Rahmen der Fernwartung anfallenden Daten ist zu untersagen.
- Für die Durchführung der Fernwartung muss eine eigenen Benutzerkennung eingerichtet werden. Das dazugehörige Passwort ist nach jedem Wartungsvorgang zu ändern.
- Bei der Fernwartung ist die Verbindung oder die Freischaltung (nach einem Authentifikationsprozess) stets vom Auftraggeber aus aufzubauen (Call-Back-Verfahren) oder frei zu geben, damit sichergestellt ist, dass keine unbefugten Einwählversuche stattfinden können. Nach Abschluss der Wartungsarbeiten ist diese Verbindung wieder zu deaktivieren.
- Vom Auftraggeber sind der Wartung/Fernwartung nur solche Zugriffsmöglichkeiten zu eröffnen, die für die Fehlerbehebung unbedingt erforderlich sind. Insbesondere gilt dies für Systemverwalterprivilegien und den Zugriff auf personenbezogene Daten. Es ist ferner darauf zu achten, dass im Rahmen der Wartung bzw. Fernwartung keine Funktionen frei geschaltet werden, die eine Übertragung oder Auswertung von Anwenderdatenbeständen zulassen. Eine Übertragung personenbezogener Daten zur Fernwartungsstelle muss auf den Einzelfall beschränkt sein und nur mit Einverständnis des Auftraggebers erfolgen können. Ein zweckwidriger Zugriff auf andere Rechner im Netz ist zu unterbinden.
- Soweit möglich müssen alle Aktivitäten im Rahmen der Fernwartung vom Auftraggeber online mitverfolgt werden. Im Zweifelsfalle muss dieser Mitarbeiter auch die Aktivitäten jederzeit abbrechen können.
- Außerdem sind alle Aktivitäten der Fernwartung (inklusive etwaiger versuchter Fernzugriffe) aufzuzeichnen und die entsprechenden Protokolle auszuwerten. Bei besonders kritischen Aktionen ist der gesamte Dialog zu protokollieren, damit später erkennbar wird, auf welche Daten zugegriffen wurde.

- Zur Sicherung der Vertraulichkeit der übertragenen Daten auf dem Übertragungswege kann es erforderlich sein, dass die Daten mit einem starken Algorithmus (mindestens 128 Bit bei symmetrischer Verschlüsselung und mindestens 1024 Bit bei asymmetrischer Verschlüsselung) verschlüsselt werden. Es ist in diesem Falle jedoch darauf zu achten, dass die Protokollierung vor Ort unverschlüsselt erfolgt und nicht auf dem Rechner des Fernwarters. Nur so ist eine effektive Kontrolle durch den Auftraggeber gewährleistet.

Zu Fragen im Zusammenhang mit einer Fernwartung in speziellen Bereichen verweise ich auf die auf meiner Homepage im Internet im Bereich Technik/Rechnersysteme unter www.datenschutz-bayern abrufbare Orientierungshilfe zur „Wartung und Fernwartung im Mainframe-Bereich“ und auf meine Ausführungen zur „Wartung medizin-technischer Anlagen“ im 19. Tätigkeitsbericht von 2000 unter Nr. 17.3.3.

Einsatz von Remote Management (Control) Programmen

Remote Management Programme (z. B. pcAnywhere oder WinTel) – auch als Remote Control Programme oder Remote Support Programme bezeichnet – ermöglichen einem Systemadministrator, von seinem Arbeitsplatz aus Zugriff auf andere im Netzwerk angeschlossene Computer zu nehmen. Dies dient hauptsächlich einer Fehlersuche und –beseitigung. Hat ein Benutzer Probleme bei der Arbeit an seinem PC und teilt dies dem Administrator mit, so kann sich dieser mit Hilfe der Fernsteuerungssoftware je nach Einstellung des Programmes entweder alles, was auf dem Bildschirm des Benutzers angezeigt wird, auch auf seinem eigenen anzeigen lassen oder zumindest auf bestimmte Programme und Daten auf dem fremden Rechner zugreifen. Zudem kann der Administrator steuernd in den Dialog eingreifen und - an Stelle des Benutzers - Eingaben tätigen, aus der Ferne Installationsarbeiten am PC des Benutzers durchführen oder sich als Administrator anmelden.

Weitere Einsatzmöglichkeiten für diese Software bestehen darin, Wartungsarbeiten an einem Server in der Dienststelle von zu Hause vorzunehmen oder auch von der Dienststelle aus bei einem Telearbeiter zu Hause Software-Updates aufzuspielen. Notwendige Wartungsarbeiten lassen sich dadurch schneller und kostengünstiger vornehmen.

Auch der Versand von Nachrichten oder das Überspielen von Daten ist auf diese Weise möglich.

Der Zugriff auf den zu bearbeitenden Rechner kann entweder über das eigene Netzwerk, über einen ISDN-Adapter, ein Modem oder mittels Browser über das Internet erfolgen.

Diese Art von Fernbedienung beinhaltet natürlich auch die Gefahr des Missbrauches. So kann sie zur Überwachung von Mitarbeitern verwenden werden, indem beispielsweise alle Tastatureingaben des Überwachten aufgezeichnet und zur Auswertung an einen anderen PC übersandt werden. Außerdem besteht die Möglichkeit, unbemerkt Dateien herunterzuladen oder aufzuspielen bzw. unberechtigt auf gespeicherte Daten zuzugreifen. Dateien oder ganze Verzeichnisse könnten kopiert, verändert, gelöscht oder umbenannt werden. Denkbar ist es auch, Passwörter auszulesen oder Veränderungen an Systemprogrammen vorzunehmen.

Ist der Einsatz einer Fernsteuerungssoftware bei einer Behörde aus dienstlichen Gründen erforderlich, so sollten zumindest folgende technisch-organisatorischen Maßnahmen getroffen werden:

- Mit dem Personalrat sollte eine Dienstvereinbarung abgeschlossen werden, in der parallel zu einer zu erlassenden Dienstanweisung die Zugriffsmöglichkeiten, Zugriffsgründe, die Zugriffsarten und die dabei zu ergreifenden Sicherheitsmaßnahmen eindeutig geregelt sind. Der **zeitlich uneingeschränkte** Zugriff auf andere Rechner ist zu untersagen. Diese Dienstanweisung muss jedem Mitarbeiter zur Kenntnis gebracht werden, der entweder die Fernzugriffe durchführt oder auf dessen PC zugegriffen werden soll.
- Die Möglichkeiten des eingesetzten Remote Management Programmes sind auf diese festgelegten Regelungen zu beschränken. So könnte beispielsweise der Zugriff auf bestimmte Rechner (z. B. in der Personalabteilung) ganz verboten oder bestimmte Verzeichnisse oder Dateien vom Zugriff ausgenommen sein. Generell ist der Zugriff auf personenbezogene Daten auf das unbedingt Notwendige zu reduzieren.
- Wann immer möglich, sollte der Bedienstete bei jedem Zugriffsversuch die Möglichkeit haben, zu entscheiden, ob er den Zugriff auf seinen PC zulässt oder nicht.
- Falls dies im Einzelfall nicht möglich ist, muss dem Betroffenen zumindest der Remote-Zugriff angezeigt werden.
- Soweit möglich hat sich der Zugreifende mittels Passwort beim Zugriffsobjekt zu legitimieren.
- Bei einem Fernzugriff von oder nach außerhalb des Netzwerkes muss gewährleistet sein, dass personenbezogene Daten nur verschlüsselt übertragen werden.

- Sollte der Verdacht bestehen, dass der Zugriff auf Daten erfolgt, die offenkundig nicht für den Wartungsfall erforderlich sind, sollte der PC-Nutzer die Möglichkeit haben, die Verbindung abzubrechen.
- Die lückenlose Protokollierung aller Zugriffsversuche muss gewährleistet sein, so dass erkennbar ist, wer mit Hilfe der Fernwirkungssoftware wann auf welche Art und Weise auf welche Daten zugegriffen hat. Diese Protokolldaten sind regelmäßig von einem nicht der Systemadministration angehörigen Mitarbeiter (z. B. behördlicher Datenschutzbeauftragter, Personalrat) auszuwerten.

17.1.10 Platform for Privacy Preferences (P3P)

Am 16.04.2002 wurde vom World Wide Web Consortium (W3C) die Platform for Privacy Preferences (P3P) Version 1.0 (http://www.w3.org/2002/04/p3p-pressrelease) als Empfehlung verabschiedet. Bei P3P Version 1.0 handelt es sich um ein einfaches, standardisiertes und automatisiertes Protokoll zur formalen und maschinenlesbaren Beschreibung von Datenschutzerklärungen (siehe auch Abschnitt 17.1.7 „Der Internet-Auftritt“). Die Diskussion um notwendige oder sinnvolle Erweiterungen sind bereits im Gange.

Grundsätze

Aufgrund der Verwendung von XML zur Formulierung einer Datenschutzerklärung kann diese zum einen automatisch in der jeweiligen Sprache des Besuchers dargestellt werden. Zum anderen kann der Besucher von seinem Browser automatisch prüfen lassen, ob eine Webseite seinen spezifischen, in seinem Browser voreingestellten Anforderungen an den Datenschutz genügt.

P3P erlaubt somit Nutzern des Internet eine bessere Kontrolle über die Nutzung ihrer personenbezogenen Daten durch die von ihnen besuchte Web-Site. Die formalisierte und dv-technisch validierbare P3P Datenschutzerklärung steht ergänzend neben den verbalen Informationen, die Telediensteanbieter aufgrund der Forderungen des Teledienste- und des Teledienstedatenschutzgesetzes den Nutzern bereit zu stellen haben. Auf meiner Homepage stelle ich seit dem 23.04.2002 meine Datenschutzerklärung auch im P3P-Format zur Verfügung.

Ob die tatsächliche Datenverarbeitung beim Telediensteanbieter allerdings mit der Ankündigung in der Datenschutzerklärung übereinstimmt, lässt sich auch mit der Validierung einer P3P Datenschutzerklärung nicht überprüfen.

Praktische Anwendung

Der Internetnutzer benötigt lediglich eine Browser-Software, die in der Lage ist, P3P Datenschutzerklärungen zu lesen und zu verarbeiten. Andere spezielle Software ist nicht erforderlich. Zum Zeitpunkt des Redaktionsschlusses unterstützte nur der Microsoft Internet Explorer (ab Version 6.0) einen Teil der P3P Empfehlung. Für andere Browser ist dies für die nahe Zukunft angekündigt.

Stehen einzelne Definitionen der P3P Datenschutzerklärung im Widerspruch zu den vom Nutzer in seinem Browser gewählten Einstellungen, z.B. bzgl. Akzeptanz von Cookies, so erscheint in der Fußzeile des Browsers ein Warnhinweis.

Im Microsoft Internet Explorer 6 gelangt man unter dem Menü "Anzeigen - Datenschutzbericht" nach dem Anzeigen von "allen Websites", der Selektion einer Seite und durch Drücken von „Zusammenfassung" schließlich zu einer lesbaren Darstellung der P3P Datenschutzerklärung - interpretiert durch den Microsoft Internet Explorer.

Wenn der Internetnutzer eine vorgefundene P3P Datenschutzerklärung überdies vom World Wide Web Consortium nach den formalen P3P Kriterien (bzgl. Syntax, Links, usw.) automatisch validiert haben möchte, so ist dies unter dem Link http://www.w3.org/P3P/validator.html durchführbar.

Folgerung

Mit der praktischen Verfügbarkeit von P3P ist ein wesentlicher Schritt in Richtung mehr Transparenz und Datenschutzschutzfreundlichkeit für den Internetnutzer getan. Es kommt jetzt darauf, dass die Browserhersteller die P3P-Funktionalität zügig in Ihre Produkte einbauen, der Standard P3P fortentwickelt wird, die Internetnutzer diese neue Möglichkeit zur Validierung von Datenschutzerklärungen nutzen und auch die Internet- und Informationsanbieter ihre Datenschutzerklärungen zusätzlich zur Textversion ebenfalls in P3P-Format bereitstellen.

17.2 Prüfungen, Beratungen und Informationen

17.2.1 Erkenntnisse aus Prüfungen

Im Berichtszeitraum habe ich bei folgenden Dienststellen die Einhaltung der gebotenen technischen und organisatorischen Datensicherheitsmaßnahmen überprüft:

- Alten- und Pflegeheim „Römerschanz“ des Bayerisches Rotes Kreuzes
- AOK-Direktion Kempten
- Bezirkskrankenhaus Taufkirchen
- Brentano-Volksschule in Aschaffenburg
- Gemeinde Altdorf
- Gemeinde Memmelsdorf
- Gemeinde Putzbrunn
- Kreiskrankenhaus Haßfurt
- Stadt Schweinfurt
- Stadt Kitzingen

Ergebnisse der Kontrolltätigkeit

Die Kontrollen ergaben, dass der Stand der technisch-organisatorischen Datensicherheitsmaßnahmen recht unterschiedlich ist. Erfreulich ist, dass bei vielen Stellen der Datenschutz und die Datensicherheit einen hohen Stellenwert besitzen, so dass nur geringfügige Lücken im Sicherheitssystem festzustellen waren. Andererseits wurden bei manchen Stellen in Teilbereichen erhebliche Defizite aufgedeckt.

Verschlüsselung bei der Datenfernverarbeitung

Obwohl ich bereits in den letzten Tätigkeitsberichten immer wieder daraufhingewiesen habe, dass personenbezogene Daten, die über das öffentliche Leitungsnetz übertragen werden, verschlüsselt werden müssen, da sonst die Vertraulichkeit der Informationen nicht gewährleistet ist und die Daten für missbräuchliche Zwecke aufgezeichnet und genutzt werden könnten, gibt es immer noch öffentliche Stellen, die zum Teil auch sensible Daten unverschlüsselt über das Internet übertragen. Im Übrigen ist auch im Rahmen der Fernwartung immer dann eine Datenverschlüsselung erforderlich, wenn auf Echtdaten zugegriffen werden muss.

Virenbekämpfungskonzept

Der Einsatz von aktuellen Virenscannern sowohl beim zentralen Datenbankserver als auch beim E-Mail-Server und – soweit vorhanden – bei der Firewall ist unverzichtbar. Auch ein laufendes Scannen der Arbeitsplatzrechner wird dringend angeraten, insbesondere wenn diese PC mit Disketten- und/oder CD-ROM-Laufwerken ausgestattet sind oder verschlüsselte Dateien erhalten. Diese Dateien müssen nach dem Entschlüsseln – wie auch jeder unverschlüsselte Anhang einer E-Mail – auf der Festplatte abgespeichert und gescannt werden und dürfen erst anschließend geöffnet werden.

Bei der Verwendung von Virensuchprogrammen verschiedener Anbieter ist zu beachten, dass diese unabhängig voneinander verwendet werden. Bei gleichzeitigem Gebrauch verschiedener, nicht aufeinander abgestimmter Produkte kann es zu falschen Virenalarmen kommen. Aufgrund des Anschlusses an öffentliche Netze müssen spezielle Virenscanner zum Einsatz gelangen, die auch Hostile Applets aufspüren können.

Die allermeisten Dienststellen setzen zwar – zumindest wenn sie über einen Internetzugang verfügen – entsprechende Software zur Bekämpfung von Viren ein, vergessen aber dabei, eine Schutzfunktion zu aktivieren, die einen Virenbefall durch verseuchte E-Mail-Anhänge verhindern kann. Viele moderne Virenscanner verfügen über die Möglichkeit, ein so genanntes „Dateiblocking“ durchzuführen. Dabei werden Dateianhänge in E-Mails nicht nur auf Viren überprüft, sondern auch bestimmte, einstellbare Dateitypen (z. B. die stets verdächtigen vbs- und exe-Dateien) in so genannten „Quarantäneordner“ abgelegt und zunächst 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. Nähere Informationen zu diesem Thema können u.a. unserer Orientierungshilfe „Sicherheitsmaßnahmen im Landkreis-Behördennetz“ auf unserer Homepage www.datenschutz-bayern.de im Bereich Technik/Orientierungshilfen/Vernetzung entnommen werden.

Online-Datenschutzprinzipien und Pflicht zur Anbieterkennung

Häufig wird übersehen, dass gemäß § 4 Abs. 1 Teledienstedatenschutzgesetz (TDDSG) jeder Nutzer einer Homepage vor der Erhebung personenbezogener Daten über Art, Umfang, Ort und

Zwecke der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten unterrichtet werden muss. Dies geschieht mit Hilfe so genannter Online-Datenschutzprinzipien (Privacy Policy). Nähere Hinweise dazu enthalten unsere gleichnamige Orientierungshilfe – abrufbar auf unserer Homepage (www.datenschutz-bayern.de) im Bereich „Technik/Grundsätze“ und das Kapitel „Der Internet-Auftritt“ in diesem Tätigkeitsbericht.

Im Übrigen besteht eine Pflicht zur Anbieterkennzeichnung gemäß § 6 Mediendienste-Staatsvertrag (MDStV) und § 6 Teledienstegesetz (TDG).

Absicherung von Serverräumen

Aufgrund der Abhängigkeit vieler öffentlicher Stellen von der ständigen Verfügbarkeit der Rechnersysteme muss Vorsorge gegen einen eventuellen Ausfall der DV getroffen werden. Dazu gehört insbesondere auch die Absicherung der Serverräume. Deshalb müssen neben der Wahl eines geeigneten Raumes Sicherheitsmaßnahmen für diesen ergriffen werden. Insbesondere sind Maßnahmen zur Zugangskontrolle (Festlegung der Zugangsberechtigungen, Außen- und Innenhautsicherung, revisionsfähige Schlüssel- und Chipkartenregelung usw.) und zur Bekämpfung von physischen Schäden (z. B. Schutz vor Feuer und Wassereinbrüchen) zu ergreifen. Näheres dazu enthält das Kapitel 17.3.8 in meinem 19. Tätigkeitsbericht.

Auswertung der Logdateien

Alle Sicherheitsverletzungen (einschließlich eventueller Eindringversuche in das Netzwerk einer öffentlichen Stelle) an den DV-Anlagen bzw. im Netzwerk sind durch Auswertung entsprechender Logdateien in einem täglichen Sicherheitsbericht aufzuzeigen und zu überprüfen, damit Sicherheitsverletzungen und vor allem Versuchen von unzulässigen Aktionen rechtzeitig nachgegangen werden kann. Die Auswertungen sind zu dokumentieren.

17.2.2 Anstieg der Beratungsleistungen

Auch in diesem Berichtszeitraum ist wiederum die Zahl der Dienststellen stark gestiegen, die sich im Vorfeld von Um- oder Neubautätigkeiten, hinsichtlich der Öffnung des lokalen Netzes zum Internet und vor der Einführung neuer DV-Verfahren mit der Bitte um Beratung bezüglich der erforderlichen Datenschutz- und Datensicherheitsmaßnahmen an meine Geschäftsstelle gewandt haben. Auch Softwareersteller, die ihre Produkte bereits in öffentlichen Bereich einsetzen

bzw. einsetzen wollen, und Sicherheitsberatungsfirmen, die Netzwerke bzw. Notfallkonzepte für Behörden planen sollen, bitten vermehrt um Anregungen bzw. legen mir ihre Konzepte zur Beurteilung vor.

Viele Kommunen möchten ihren Bürgern mit Hilfe einer serviceorientierten Verwaltung längere Wartezeiten in den Fachämtern ersparen und eine bessere Beratung bieten. Aus diesem Grunde entstehen immer mehr so genannte „Bürgerbüros“ als zentrale Anlaufstelle für die Gemeindemitglieder bzw. mit Hilfe der elektronisch gestützten Verwaltung (eGovernment) soll den Bürgern die Möglichkeit gegeben werden, ihre Behördengänge auf elektronischem Wege zu erledigen. Ein Schwerpunkt meiner Beratungstätigkeit im kommunalen Bereich lag daher darin, den Gemeinden die damit verbundenen Gefahren für den Datenschutz und die Datensicherheit aufzuzeigen und entsprechende Sicherheitsmaßnahmen vorzuschlagen.

Soweit es mir aus personellen und zeitlichen Gründen möglich ist, komme ich Beratungswünschen gerne nach, da es mir zum Einen zeigt, dass bei den Hilfe suchenden Stellen ein Datenschutzbewusstsein vorhanden ist und mir zum Anderen die Möglichkeit gegeben wird, auf eventuelle Fehler im Datenschutz- und Datensicherheitskonzept hinzuweisen. Eine wesentliche Voraussetzung für meine Beratungsleistung ist allerdings, dass ein solches Datenschutz- und Datensicherheitskonzept bereits erstellt, dem örtlich zuständigen Datenschutzbeauftragten vorgelegt und von diesem auch beurteilt wurde und erst dann mir vorgelegt wird. Die erstmalige Erarbeitung eines Datenschutz- und Datensicherheitskonzeptes kann von meiner Dienststelle aus den oben erwähnten personellen und zeitlichen Gründen beim besten Willen nicht geleistet werden.

17.3 Technische Einzelprobleme

17.3.1 Protokollauswertung auf Servern und Firewall-Systemen

Jeder Internetdienstanbieter kann über automatisch generierte Protokolle auf seinen Servern eine große Anzahl an Daten über das Verhalten seiner Nutzer gewinnen. Da das Internet für einen immer größeren Bevölkerungsanteil an immer mehr Orten zur Verfügung steht, werden auch diese Daten wertvoller und vollständiger erfassbar.

Deshalb ist besonders darauf zu achten, dass alle Protokollierungen von personenbezogenen Daten mit den entsprechenden Datenschutzvorschriften übereinstimmen.

Aus technischer Sicht werden Protokolle bei der Internetnutzung hauptsächlich zum Erkennen von Fehlern und Angriffen und zur Optimierung von Netzdiensten verwendet. Auch für die eventuelle Abrechnung der Dienstnutzung sind Protokolldaten unumgänglich.

Nach § 3 Abs. 1 und § 6 Abs. 1 Teledienstedatenschutzgesetz (TDDSG) ist es dem Diensteanbieter in Deutschland nur erlaubt, personenbezogene Daten über die Inanspruchnahme von Telediensten zu erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen (Nutzungsdaten) oder um die Nutzung von Telediensten abzurechnen (Abrechnungsdaten).

Protokollauswertung auf Firewallsystemen

Da beim Einsatz einer Paket-Firewall der gesamte Internetverkehr zwischen internem und externem Netz durch die Firewall fließt und dort auf Zulässigkeit geprüft wird, können hier besonders viele Daten in Logdateien gespeichert werden. Für jedes einzelne Datenpaket kann hier mitprotokolliert werden:

- Absende IP Adresse und Absende Port
- Empfänger IP Adresse und Empfänger Port
- Erlaubnis, Zurückweisung oder Unterdrückung der Verbindung
- Protokolldetails

Nicht protokolliert wird in der Regel der Inhalt der einzelnen Pakete.

Da zumindest eine IP Adresse innerhalb des eigenen Netzes liegt, kann diese auch einem internen Nutzer zugewiesen und somit personenbezogen sein. Aber auch die IP Adressen von außerhalb können, zumindest in Kombination mit Informationen aus anderen Datenbanken, eventuell einzeln bestimmbaren Personen zugeordnet werden.

Eine Protokollierung auf einer Firewall wird vorgenommen, um die Sicherheit des eigenen Netzes zu überwachen und auf Einbruchsversuche reagieren zu können. Aus Sicherheitsgründen ist

deshalb eine Protokollierung nach dem allgemeinen Datenschutzgesetzen durchaus möglich. Zur Erkennung von Langzeitangriffen halte ich einen Zeitraum von maximal drei Monaten für die Aufbewahrung und Verwendung der Logdateien für akzeptierbar. Hierbei ist jedoch eine strikte Zweckbindung zu beachten.

Sollen die Logdateien auf einer Firewall auch für statistische Zwecke verwendet werden, so müssen dafür die vollständigen IP Adressen mindestens durch Wegkürzen der letzten drei Stellen anonymisiert werden. Danach handelt es sich um keine personenbezogenen Daten mehr und damit unterliegen sie auch keinen datenschutzrechtlichen Restriktionen mehr.

Zu prüfen ist auch, ob es nicht reicht, für die Gewährleistung der Sicherheit ein bestimmten, nicht zulässigen Teil des Verkehrs zu protokollieren (Datensparsamkeit).

Neben einer Paket-Firewall werden in der Regel auch auf der Anwendungsebene Programme eingesetzt, die die Kommunikation zwischen internem und externem Netz ermöglichen. Dies kann zum Beispiel ein Mail-Server oder Proxy-Server sein. Auf diesen Servern kann nicht nur der Aufbau einer Verbindung zwischen zwei IP Adressen protokolliert werden, sondern beispielsweise auch, wer mit wem E-Mails ausgetauscht hat und welche IP Adresse welche WWW-URLs besucht hat.

Da diese Daten normalerweise nicht für Abrechnungszwecke verwendet werden, dürfen sie nur zu Betriebszwecken gespeichert und verwendet werden. Da die zuverlässige Übermittlung von E-Mails einerseits auch das Suchen von länger zurückliegenden Fehlern nötig machen kann und andererseits der Mailserver auch Angriffen von Außen ausgesetzt ist, betrachte ich hier eine strikt zweckgebundene Speicherung von bis zu drei Monaten für zulässig. Für einen Proxy fallen keine sicherheitsrelevanten Protokolldaten an, deshalb müssen die Daten so schnell wie möglich, spätestens jedoch nach einem Tag gelöscht oder anonymisiert werden - falls sich die Protokollierung nicht gänzlich unterbinden lässt, was immer zu bevorzugen ist.

Protokollauswertung auf Webservern

Neben den Diensteanbietern haben auch die Inhaltsanbieter im Internet ein großes Interesse an Daten über die Nutzung ihres Angebots und das Surf-Verhalten der Dienstenutzer. Ein Webserver, der die einzelnen Webseiten an die Nutzer ausliefert, protokolliert in der Standardkonfigu-

ration die abgerufene URL, die anfordernde IP Adresse, den Browser und das Betriebssystem des Nutzers sowie eventuell an den Server übergebene Argumente wie etwa die Daten, die in einem Formular eingegeben wurden.

Grundsätzlich ist auch hier ist die IP Adresse, unabhängig davon, ob sie dynamisch vergeben oder statisch ist, als personenbezogen zu betrachten. Sowohl dynamische also auch statische IP Adressen können vom jeweiligen Netzblock Eigentümer in der Regel einer Person oder zumindest einem Telefon- oder DSL-anschluss zugeordnet werden. Sollen Auswertungen über den Nutzungsgrad des Internetauftritts gefertigt werden, so ist die Speicherung der vollständigen IP Adresse hierzu nicht erforderlich, das heißt sie ist nicht zulässig. Da die meisten Web-Server nur eine vollständige Protokollierung der IP Adressen oder überhaupt keine Protokollierung zulassen, ist es jedoch akzeptierbar, wenn die Datensätze, etwa durch Wegkürzen der drei letzten Stellen, täglich anonymisiert werden.

17.3.2 Einsatz von Videotechnik

In früheren Tätigkeitsberichten habe ich mich bereits zu Fragen

- der Videoüberwachung kommunaler Wertstoffhöfe und Containerstandorte (vgl. 18. TB, Ziff. 18.1),
- der Bildaufnahmen bei Versammlungen durch die Polizei (vgl. 19. TB, Ziff. 5.6.3),
- der Videoüberwachung öffentlicher Straßen und Plätze durch die Polizei (vgl. 19. TB, Ziff. 5.6.4) und
- der Videoüberwachung öffentlicher Plätze durch Kommunen (vgl. 19. TB, Ziff. 8.8) geäußert.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Rahmen ihrer 59. Sitzung vom 14./15.03.2000 in der Entschließung „Risiken und Grenzen der Videoüberwachung“ mit dem Themenkomplex befasst und Grundsätze hierzu aufgestellt.

Und auch in diesem Berichtszeitraum wurde ich mehrfach zum Einsatz optisch-elektronischer Überwachungseinrichtungen um Beratung gebeten, so z.B.

- von einer Gemeinde zur Videoüberwachung ihres Friedhofes nach z.T. erheblichen Sachbeschädigungen und sonstigen nachhaltigen Störungen der Totenruhe,
- von einer meiner Kontrollkompetenz unterliegenden Einrichtung im Rahmen der Außensicherung ihrer Liegenschaften (insbesondere außerhalb der Dienstzeiten),
- von mehreren Schulen zur Überwachung ihres Eingangsbereichs zum Schutz vor Zutritt durch Unbefugte und
- von einer Universität zur Überwachung Ihrer CIP-Räume nach Diebstahlsvorfällen und zur Fertigung von Mitschnitten von Vorlesungen für weitere Informations- und Schulungszwecke.

Nun besteht die Schwierigkeit, dass in den o.g. Fällen einerseits keine bereichsspezifischen Regelungen - vergleichbar dem Einsatz von Videotechnik im Polizeibereich - bestehen und auch das Bayerische Datenschutzgesetz im Gegensatz zum Bundesdatenschutzgesetz (vgl. § 6 b BDSG) keine spezielle Rechtsnorm enthält. Da es sich bei Videoüberwachung aber um eine Datenerhebung handelt, bleibt als Prüfungsmaßstab mangels einer speziellen Norm nur Art. 16 BayDSG.

Aus Gründen der Prävention, der Gefahrenabwehr und zum Schutz des öffentlichen Eigentums halte ich Videoüberwachungen in den o.g. Fällen für akzeptabel, sofern nachfolgende Voraussetzungen erfüllt sind:

- Die Videoüberwachung dient der Verhinderung oder Verfolgung von Eigentumsstörungen und/oder sonstiger strafrechtlich relevanter Ereignisse und findet im Rahmen der Ausübung des Hausrechts statt.

- Ist keiner der vorstehenden Zwecke gegeben – wie teilweise im obigen vierten Fall (Vorlesungsmitschnitte) – so kommt nur eine rechtswirksame Einwilligung der Betroffenen in Betracht. Zu deren praktischer Erreichbarkeit habe ich aber gerade im Bereich einer Vielzahl von möglichen Betroffenen – z.B. Hörer von Vorlesungen – meine Zweifel.

- Die Videoüberwachung ist räumlich eng auf diejenigen Bereiche zu begrenzen, bei denen aufgrund der Erfahrungen der Vergangenheit auch künftig mit vergleichbaren Vorkommnissen (z.B. Diebstahl, Sachbeschädigung) gerechnet werden muss.

- Der Zeitraum für eine Videoüberwachung ist auf das unabdingbare Maß zu beschränken, d.h. sie erfolgt nur zu den Zeiten, in denen nach den bisherigen Erfahrungen mit einem Schadensfall gerechnet werden muss, also z.B. im o.g. Fall des Friedhofs nur nachts zu den Zeiten, in denen das Betreten des Friedhofs nicht erlaubt ist.

- Gemäß Art. 16 Abs. 2 Satz 1 BayDSG sind personenbezogene Daten primär beim Betroffenen mit dessen Kenntnis zu erheben. Auf die Videoüberwachung ist deshalb durch entsprechende Hinweisschilder deutlich hinzuweisen, auf denen der Erhebungszweck anzugeben ist (vgl. Art. 16 Abs. 3 Satz 1 BayDSG).

- Die Aufzeichnungen unterliegen einer strikten Zweckbindung und dürfen nur zur Täterfeststellung und/oder zur Beweissicherung ausgewertet werden. Sie sind zu löschen (möglichst automatisch), sobald sie hierzu nicht mehr erforderlich sind. Die maximale Speicherdauer für Aufzeichnungen ist möglichst kurz zu fassen, also z.B. auf 36 Stunden im o.g. Fall des gemeindlichen Friedhofs oder auf drei Schultage im Falle der o.g. Schulen.

- Sind die Kameraeinrichtungen schwenkbar und evtl. überdies zoombar ausgelegt, so ist darauf zu achten, dass keine schutzwürdigen Belange eigener Bediensteter betroffen werden (z.B. zoomendes Schwenken mit Blick in Diensträume hinein). Dies kann je nach verwendetem System z.B. durch technische Beschränkung der Nutzbarkeit von Zoom- und Schwenkfunktion auf Zeiträume außerhalb der Dienstzeiten und/oder durch softwaretechnisches Sperren bestimmter möglicher Beobachtungsbereiche (Ausblenden) erreicht werden.

- Es sind geeignete Sicherungsmaßnahmen vor einem unberechtigten Zugang und Zugriff zu den Aufzeichnungsgeräten und zu den Aufzeichnungen zu ergreifen.

- Es sind entsprechende schriftliche Regelungen und Festlegungen zu treffen.

Das Bayerische Staatsministerium für Unterricht und Kultus hat auch als Reaktion auf meine Beratung mehrerer Schulen in einem Informationsschreiben alle Schularten über die o.g. Grundsätze zur Videoüberwachung schriftlich unterrichtet. Ich begrüße diese Maßnahme.

17.3.3 Outsourcing von Kommunaldaten

Im vergangenen Jahr sind einige Kommunen an mich herangetreten, mit der Bitte um Auskunft, ob eine Gemeinde berechtigt sei, personenbezogene Daten in ein privat betriebenes Rechenzentrum auszulagern. Ebenfalls Unklarheit herrschte darüber, in wieweit einzelne DV-Leistungen (z. B. Systemverwaltung) ausgelagert werden können.

Outsourcing der Datenbankserver mit dem gesamten Datenbestand

Art. 6 des Bayerischen Datenschutzgesetzes (BayDSG) enthält Regelungen, die bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag zu beachten sind. Im Umkehrschluss kann daraus entnommen werden, dass sich eine öffentliche Stelle bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten grundsätzlich einer anderen Stelle bedienen darf, wobei vom Gesetzgeber keine Einschränkung zu Lasten lediglich öffentlicher Auftragnehmer getroffen wurde. Voraussetzung ist jedoch, dass keine Funktionsübertragung stattfindet, das heißt die Aufgabe selbst, zu deren Wahrnehmung die Erhebung, Verarbeitung oder Nutzung dient, muss beim Auftraggeber verbleiben (Wilde/Ehmann/Niese/ Knoblauch, Bayerisches Datenschutzgesetz Art. 6, Rdnr. 10). Die Erhebung, Verarbeitung oder Nutzung von Daten, mit der die andere Stelle beauftragt wird, darf somit im Ergebnis lediglich in einer Hilfstätigkeit bestehen.

Bei der Auftragsdatenverarbeitung bleibt wie unter Nr. 17.1.5. – Auftragsdatenverarbeitung (Outsourcing) – dargelegt, der Auftraggeber für die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die im zweiten Abschnitt des Bayerischen Datenschutzgesetzes genannten Rechte, zum Beispiel das Auskunftsrecht des Betroffenen, sind ihm gegenüber geltend zu machen (Art. 6 Abs. 1 BayDSG). Nach Art. 6 Abs. 2 BayDSG ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

Ich halte die Vorhaltung personenbezogener Daten von Kommunen in einer Datenbank eines privaten Rechenzentrumsbetreibers im Rahmen der Auftragsdatenverarbeitung unter Beachtung

der oben dargestellten Grundsätze und unter Beachtung der nachstehenden Ausnahmen generell für zulässig, wenn auch nicht unbedingt für wünschenswert, da sich die Gefahr erhöht, dass Unberechtigte auf die den Gemeinden größtenteils gezwungenermaßen und nicht freiwillig anvertrauten Daten der Bürger Zugriff nehmen können.

Ich weise jedoch darauf hin, dass für bestimmte Daten spezielle gesetzliche Bestimmungen eine Datenverarbeitung im Auftrag ausschließen. So können nach Art. 36 Abs. 1 Satz 1 des Bayerischen Meldegesetzes **Meldebehörden** lediglich andere Gemeinden oder die Anstalt für kommunale Datenverarbeitung in Bayern mit der Erfüllung der Aufgaben nach dem Bayerischen Meldegesetz und den aufgrund dieses Gesetzes erlassenen Rechtsvorschriften mit Hilfe automatisierter Verfahren beauftragt werden. Diese Regelung schließt zwar die Möglichkeit nicht aus, sich zur Erfüllung einzelner Datenverarbeitungsaufgaben, wie zum Beispiel der Erfassung von Daten, privater Institutionen zu bedienen, soweit dabei die Voraussetzungen des Bayerischen Meldegesetzes und des Bayerischen Datenschutzgesetzes beachtet werden, die Beauftragung privater Auftragnehmer mit der Erfüllung **aller** mit der automatisierten Führung des **Melderegisters** zusammenhängenden Aufgaben ist danach jedoch nicht möglich. Gleiches gilt gemäß Art. 80 Abs. 5 Nr. 2 SGB X für die **Sozialdatenverarbeitung** im Auftrag. Auch hier darf der Auftrag nicht die **gesamte** Speicherung des Datenbestandes umfassen.

Soweit die Speicherung der im vorherigen Absatz erwähnten Datenbestände von der Auftragsdatenverarbeitung ausgenommen werden würde, müsste darauf geachtet werden, dass eine Kenntnisnahme und ein Zugriff auf andere sensible Datenbestände durch den Auftragnehmer (insbesondere im Rahmen der durch den Auftragnehmer übernommen Systemadministratortätigkeiten) im Hinblick auf die schutzwürdigen Belange der Betroffenen durch **Verschlüsselung** auszuschließen ist. Dies gilt z. B. für folgende Datenbestände:

- aus dem Steueramt (§ 30 AO – Steuergeheimnis),
- aus dem Personalbereich (Art. 100 ff. BayBG –Vertraulichkeit der Personalakte),
- für Datenbestände, die der ärztlichen Schweigepflicht unterliegen (§ 203 StGB – Patientengeheimnis),
- für Personenstandsdaten (§ 61 PStG – eingeschränktes Einsichtsrecht),
- aber auch für Daten in Vollstreckungsangelegenheiten und sonstigen Verwaltungsverfahren, die nach Art. 30 BayVwVfG geheim zu halten sind.

Die einzige Möglichkeit, die ich derzeit für eine komplette Auslagerung der Kommunaldaten sehe, besteht darin, einen Raum beim Outsourcingpartner anzumieten und dort die Server der Kommune aufzustellen. Die Verfügungsgewalt über diesen Raum muss ausschließlich beim Mieter liegen. Außerdem muss der Vermieter ausdrücklich auf das ihm sonst nach dem BGB zustehende Vermieterpfandrecht verzichten. Zur Gewährleistung der Zugangssicherheit zum angemieteten Serverraum müsse Maßnahmen zur Innen- und Außensicherung wie Installation einer Einbruchmeldeanlage an Fenster und Türen, Ausstattung der Türe des Serverraums mit mechanischem Türschließer, Zylinderschloss und Türknauf ergriffen werden. Für die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität für die gespeicherten und zu übermittelnden Daten müssen zusätzliche Maßnahmen (z. B. Verschlüsselung – siehe Zentrale Datenbank verschiedener Gemeinden und Auslagerung der Systemadministration) ergriffen werden.

Zentrale Datenbank für mehrere Gemeinden

Bei der Vorhaltung personenbezogener Daten verschiedener Gemeinden in einer zentralen Datenbank ist zusätzlich zu den oben genannten Maßnahmen darauf zu achten, dass die Datenbestände zumindest logisch getrennt voneinander gespeichert werden. Die Anlegung einer einzigen Datei für alle Gemeinden ist unzulässig, soweit eine solche nicht ausdrücklich vom Gesetz vorgesehen ist. Sie ist aus datenschutzrechtlicher Sicht auch insoweit abzulehnen, als ein Missbrauch einer solchen Datei regelmäßig schwerwiegender ist als der der Datei einer einzelnen Gemeinde, da sie einen wesentlich umfassenderen Datenbestand aufweist. Aus allgemeinen datenschutzrechtlichen Überlegungen heraus ist es zudem wünschenswert, zentrale Datensammlungen möglichst zu verhindern bzw. soweit sie sich nicht vermeiden lassen, ihre Zahl möglichst gering zu halten, da sie eine erhöhte Gefahr in sich bergen, unzulässigerweise oder gegebenenfalls auch nach Schaffung einer entsprechenden Rechtsgrundlage für andere Zwecke als den, zu dem sie angelegt wurden, genutzt zu werden.

Der Zugriff auf die Daten ist darüber hinaus insoweit zu beschränken, als jede Kommune nur ihre eigenen Daten abrufen kann, da die Zuständigkeit nicht über das jeweilige Hoheitsgebiet hinaus reicht. Sollten im Einzelfall Daten einer anderen Gemeinde zur Erfüllung einer bestimmten Aufgabe notwendig sein, können diese unter Berücksichtigung der einschlägigen datenschutzrechtlichen Vorschriften übermittelt werden.

Außerdem weise ich darauf hin, dass durch ausreichende technische und organisatorische Maßnahmen sicherzustellen ist, dass die Vorschriften des Bayerischen Datenschutzgesetzes und anderer Gesetze über den Datenschutz eingehalten werden. Dazu gehört zum Beispiel, dass geeignete Vorkehrungen getroffen werden, um einen Zugriff unbefugter Dritter auf die gespeicherten Daten zu verhindern. Außerdem ist zur Wahrung der Vertraulichkeit und Integrität der Daten eine Verschlüsselung der Daten auf dem Übertragungsweg, der bedingt ist durch die räumliche Trennung des Rechners von der Gemeindeverwaltung, zwingend erforderlich. 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. Zur Durchführung der Verschlüsselung bietet sich die Einrichtung eines virtuellen privaten Netzes (VPN) an. Ein VPN ist ein privates Netzwerk, welches von der öffentlichen Telekommunikationsstruktur Gebrauch macht, gleichzeitig die Privatsphäre durch den Einsatz von so genannten Tunnelling- und Sicherheitsprotokollen schützt und in der Regel über das Internet realisiert wird. Virtuell bedeutet dabei, dass der Anwender glaubt, seine Daten laufen über exklusive (private) Verbindungen. In Wirklichkeit wird die vorhandene Netzstruktur jedoch – aus Kostengründen – von verschiedenen Anwendern gemeinsam genutzt.

Neben den allgemein bekannten Sicherheitsmaßnahmen (z. B. rigorose Einschränkung der Zugriffs- und Nutzungsrechte auf das unbedingt Notwendige, Ergreifung von Maßnahmen zur Virenbekämpfung, Auswertung von Sicherheitsverletzungen in den maschinell geführten Protokollen und effektiver Passwortschutz - siehe Orientierungshilfe zur „Passwortvergabe, -wahl und –verwaltung“, abrufbar auf meiner Homepage www.datenschutz-bayern.de im Bereich Technik/Orientierungshilfen/Allgemeines) müssen zur Absicherung der Gemeindedaten zusätzliche Maßnahmen ergriffen werden. So müssen beispielsweise alle Server durch Maßnahmen der Zugangskontrolle physisch geschützt werden. Die Datenzugriffe auf Server und insbesondere die Nutzung administrativer Berechtigungen müssen intensiv mit Hilfe der Protokollierung überwacht werden. Sonstige Hinweise zur Protokollierung enthält die Orientierungshilfen „Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)“ auf der Homepage des Bayerischen Landesbeauftragten für den Datenschutz.

Natürlich ist es im Rahmen der Auftragskontrolle auch erforderlich, dass sich die Gemeinde davon überzeugt, dass der Auftragnehmer die Datensicherheit durch Ergreifung der oben angeführten Datensicherheitsmaßnahmen gewährleistet.

Auslagerung lediglich der Systemadministration

Eine ledigliche Übernahme der Systemadministration der Server und die Überwachung des lokalen Netzwerkes einer Kommune mittels **Fernwartung** durch eine Privatfirma ist insbesondere dann nicht als Teilaspekt der Speicherung und sonstigen Verarbeitung von personenbezogenen Daten anzusehen, wenn den Systemadministratoren im Normalbetrieb keinerlei Zugriff auf die gespeicherten personenbezogenen Daten gestattet ist. Aufgabe der Systemadministration ist die Herstellung und Aufrechterhaltung des ordnungsgemäßen Betriebs der DV-Anlagen, nicht aber die fachspezifische Verarbeitung personenbezogener Daten. So könnte beispielsweise die Datenbankadministration durch eigenes Personal des Kunden erfolgen. Damit ist auch für Meldedaten und Sozialdaten der Begriff der Datenverarbeitung im Auftrag (Art. 6 BayDSG) nicht erfüllt. Die Privatfirma wird nicht Auftragnehmer im Sinne des Bayerischen Datenschutzgesetzes. Zur ausreichenden Wahrung der Belange des Betroffenen sieht Art. 6 Abs. 4 BayDSG i. d. F. des Änderungsgesetzes vom 25.10.2000 (GVBl. S. 752) wegen der ähnlich gelagerten Interessenlage jedoch die entsprechende Geltung der Absätze 1 bis 3 dieser Vorschrift vor. Damit ist gemäß Art. 6 Abs. 2 BayDSG insbesondere der Auftrag schriftlich zu erteilen, wobei u.a. die technischen und organisatorischen Maßnahmen festzulegen sind. Unbedingt erforderlich sind insbesondere Maßnahmen zur:

- Zugangskontrolle (z. B. Identifikation und Authentisierung, sicherer Verbindungsaufbau mittels Call Back-Verfahren über eine Firewall, dedizierte Vergabe von Zugriffsrechten und Wartungsprivilegien, Protokollierung aller Zugriffe, Ergreifung von Maßnahmen beim Zugriff auf Kundendaten)
- Wahrung der Vertraulichkeit (z. B. Einsatz von Datenverschlüsselungskomponenten bei der Datenspeicherung und der Datenübertragung, Errichtung von „Virtuellen Privaten Netzen“)
- Kundenkontrollmaßnahmen (z. B. Kontrolle der Wartungsaktivitäten online oder mittels ausgewerteter Wartungsprotokolle, ggf. Unterbrechungsmöglichkeit der Fernwartung)
- Organisatorische Maßnahmen (z. B. Einhaltung der Verschwiegenheitsvorschriften, schriftliche Festlegung der Wartungsaktivitäten, Kontrolle der Protokolle)

Da im Gegensatz zu einer reinen Hard- bzw. Softwarefernwartung hier die Systemadministrierung durch den Dritten erfolgt, ist neben einer Datenverschlüsselung insbesondere Wert auf eine umfassende Protokollierung aller Systemaktivitäten und Fernwartungszugriffe zu legen. Aus den Protokollen muss sich die Frage beantworten lassen: „Wer hat wann mit welchen Mitteln was

veranlasst bzw. worauf zugegriffen?“ Außerdem müssen sich Systemzustände ableiten lassen: „Wer hatte von wann bis wann welche Zugriffsrechte?“ Folgende Aktivitäten sind zur Überwachung der Systemadministrations- und Fernwartungsaktivitäten vollständig zu protokollieren:

- Systemgenerierung und Modifikation von Systemparametern
- Einrichten von Benutzern
- Verwaltung von Befugnistabellen
- Änderungen an der Dateiorganisation
- Durchführung von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen
- Aufruf von Administrations-Tools
- Versuche unbefugten Einloggens sowie die Überschreitung von Befugnissen
- Datenübertragungen
- Benutzung von automatisierten Abrufverfahren
- Eingabe, Veränderung und Löschung von Daten durch den Auftragnehmer
- Aufruf von besonders „sensiblen“ Programmen

Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss gewährleistet werden. Das Gleiche gilt für die Manipulationssicherheit der Einträge in den Protokolldateien. Die Protokolle müssen durch den Auftraggeber ausgewertet werden. Dazu sind sie so zu gestalten, dass eine effektive Überprüfung möglich ist.

Im Übrigen möchte ich darauf hinweisen, dass bei einer Auslagerung von Systemadministrationstätigkeiten an eine Privatfirma die Aufrechterhaltung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlagen, z.B. im Falle eines Streiks beim Auftragnehmer, nicht immer gewährleistet ist.

17.3.4 OK.FIS

Im Berichtszeitraum sind mehrere Städte an mich mit der Bitte herangetreten, zu prüfen, ob das Finanzinformationssystem OK.FIS der AKDB datenschutzrechtlich unbedenklich sei. Hauptkritikpunkt war, dass alle Anordnungsdienststellen einer Stadt Zugriff auf alle Finanzadressen (FAD) dieser Kommune hatten. So konnten alle Mitarbeiter neben der Wohnanschrift auch alle

anderen Daten – wie Bankverbindungen oder Immobilienobjekte – sowohl von Bürgern als auch von Bediensteten einsehen.

Ich habe deshalb mit Vertretern der AKDB ein Gespräch bezüglich der Datenschutz- und Datensicherheitsmaßnahmen im OK.FIS-Verfahren geführt. Dabei hat sich herausgestellt, dass der Zugriff auf die Adressdatenbank in der sich im Einsatz befindlichen Version des Verfahrens nicht detailliert geregelt war. Entweder besaß ein Mitarbeiter den Zugriff auf die Adressdatenbank mit allen darin befindlichen Daten oder er besaß keinerlei Zugriffsrechte. Eine Begrenzung des Zugriffs auf lediglich die Daten seines Sachbereichs oder einzelne Adressen bzw. Adressangaben war bei der eingesetzten Verfahrensversion nicht möglich. Damit konnte jeder Nutzer der Adressdatenbank auf alle Finanzdaten, Bankverbindungen und i.d.R. auf die zugeordneten Objekte zugreifen.

Außerdem bestand die Gefahr der Eintragung einer nicht gewünschten Bankverbindung. Hatte der Betroffene gegenüber der sachbearbeitenden Stelle eine Bankverbindung bekannt gegeben, so wurde diese vom Sachbearbeiter eingetragen. War der sachbearbeitenden Stelle die Bankverbindung nicht bekannt oder unterblieb der Eintrag des gewünschten Kontos, so wurde – soweit sie der Kasse bekannt war – von dieser die Bankverbindung (oder eine der bekannten Bankverbindungen) beim Zahlungsverkehr eingetragen. Dies konnte dann dazu führen, dass Zahlungen auf ein anderes als das gewünschte Konto erfolgte. War auch der Kasse kein Konto bekannt, wurde der Betroffene angeschrieben. Dieses daraufhin mitgeteilte Konto wurde – soweit vom Betroffenen nicht anders gewünscht – für alle Zahlungen genutzt.

Weiterhin bestand bei der zum Zeitpunkt des Gespräches eingesetzten Version des Verfahrens keine Möglichkeit, (nicht mehr benötigte) Finanzadressen oder einer Adresse zugewiesene Objekte zu löschen oder zu sperren. Damit konnten sich beispielsweise auch die Daten bereits verstorbener Bürger noch im Datenpool befinden.

Alles dies war nicht datenschutzgerecht.

Den Vertretern der AKDB unterbreitete ich im Rahmen des erwähnten Gespräches folgende Forderungen:

- Anpassung einer neuen Programmversion an die Rechtslage (kein gemeinsamer Zugriff auf die Adressdatenbank und die zugewiesenen Objekte). Jede Adresse darf nur dem berechtigten Personenkreis zugänglich sein.
- Die Vergabe der Benutzerberechtigungen und Zugriffsrechte für das Verfahren muss revisionsfähig erfolgen.
- Es muss aus Revisionsgründen jederzeit nachvollziehbar sein, wer welches Datenfeld ausgefüllt bzw. geändert hat (Protokollierung).
- Nach einer durchgeführten Jahresabrechnung und Archivierung des Altbestandes sollte die Möglichkeit bestehen, alle Finanzadressen ohne aktuelle Objekte zu löschen. Auf diese Möglichkeit der automatischen Löschung muss der Kunde der AKDB (z. B. Gemeinde) hingewiesen werden. Die Entscheidung über die Löschung verbleibt dann bei diesem Kunden.
- Alle einer Finanzadresse zugewiesenen Objekte müssen vom jeweils zuständigen Sachbearbeiter gelöscht werden können.
- Sind verschiedene Objekte einer sachbearbeitenden Stelle zugeordnet, muss die Möglichkeit geschaffen werden, den Zugriff einzelner Mitarbeiter dieser Stelle auf einzelne dieser Objekte zu beschränken (z. B. Abgrenzung Personalabteilung/Beihilfesachbearbeitung).

Mit Ausnahme der Revisionsfähigkeit der Benutzerverwaltung und der Protokollierung der Datenzugriffe wurden inzwischen alle meine Forderungen durch die AKDB erfüllt, so dass nach derzeitigem Kenntnisstand keine datenschutzrechtlichen Bedenken gegen die neue Version des OK.FIS-Verfahrens bestehen. Ich gehe allerdings davon aus, dass die entsprechenden Protokollierungskomponenten schnellstmöglich in das Verfahren integriert werden.

17.3.5 Zugriff auf das amtliche Liegenschaftsbuch

Im Berichtszeitraum wurde von der Bayerischen Vermessungsverwaltung das Auswertesystem ALB-Online entwickelt, welches zur Erteilung amtlicher Auskünfte sowie für die Datenauswertung anderer Behörden (insbesondere der Kommunen) genutzt werden kann und einen Zugriff auf die Daten des ALB (Automatisiertes Liegenschaftsbuch) einschließlich der Digitalen Flurkarte ermöglicht. Zu der Einrichtung eines automatisierten Abrufverfahrens nach Art. 8 BayDSG durch die Bayerische Vermessensverwaltung hatte ich bereits im Jahre 1998 in einer Korrespondenz mit der Bayerischen Staatskanzlei und dem Bayerischen Landkreistag die Auffassung ver-

treten, dass bei der Einrichtung eines solchen Verfahrens die schutzwürdigen Interessen der Betroffenen berücksichtigt sein müssen und der Zugriff auf die Daten zur Wahrnehmung einer konkreten Aufgabe erforderlich sein muss. Eine Weitergabe sämtlicher Daten des Liegenschaftsbuches für unbestimmte, vorher nicht absehbare Zwecke, habe ich als eine „Datenverarbeitung auf Vorrat“ abgelehnt.

Im Rahmen eines Pilotversuches wurde dem Landratsamt Starnberg für projektbezogene Einzelfälle der Online-Abruf (z. B. für Abfragen bei Altlastenverdachtsfällen, für Abfragen bei der Überprüfung von Anlagen nach der Verordnung zum Umgang mit wassergefährdenden Stoffen (VAwS) und für Abfragen bei der Einleitung von Pflegemaßnahmen) von personenbezogenen Daten aus dem ALB gestattet. Meine Geschäftsstelle wirkte dabei von Beginn an bezüglich der Fragen zum Datenschutz und zur Datensicherheit beratend mit. Sowohl die Bayerische Vermessungsverwaltung als auch das Pilot-Landratsamt waren für meine Anregungen und Forderungen aufgeschlossen.

Von Anfang an wurde darauf geachtet, dass lediglich ein begrenzter Personenkreis des Landratsamtes ALB-Anfragen starten kann. Diese Personen müssen mit Angabe des Namens, Vornamens, der Dienstbezeichnung und der E-Mail-Adresse der BFD München zur Einrichtung der Zugriffsrechte mitgeteilt werden.

Zur Identifizierung und Authentifizierung muss sich ein Anwender mittels Eingabe einer Benutzerkennung und eines Passwortes legitimieren. Dabei ist jeder Benutzer bei seiner Erstanmeldung gezwungen, das ihm mitgeteilte Transportpasswort in ein nur ihm bekanntes persönliches Kennwort zu ändern. Unsere Forderungen bezüglich der Passwortvergabe, -wahl und -verwaltung (siehe die gleichnamige Orientierungshilfe auf unserer Homepage www.datenschutz-bayern.de im Bereich Technik/Orientierungshilfen/Allgemeines) werden beachtet.

Die Datenanfrage erfolgt über eine gesicherte SSL-Verbindung (128 Bit-Verschlüsselung). Dabei muss bei jeder Abfrage ein Grund angegeben werden. Die **zugelassenen Gründe** sind in einem Katalog definiert. Das Abfrageergebnis wird sodann als verschlüsselter Dateianhang (asymmetrische Verschlüsselung mittels PGP – Schlüssellänge: 1024 Bit) vom Server des Bayerischen Vermessungsamtes per E-Mail an die jeweilige persönliche Mailbox des autorisierten Benutzers gesandt, wobei vom Server als Mailadresse diejenige ausgewählt wird, die bei der Vermessungsverwaltung als zu der betreffenden Benutzerkennung gehörend gespeichert ist. Durch

dieses Sicherheitsmerkmal können unbefugte Zugriffsversuche entdeckt und unberechtigte Datenzugriffe verhindert werden. Die Daten können dann in anderen DV-Programmen weiterverarbeitet werden.

Die BFD München führt ein automatisiertes Zugriffsprotokoll, in dem Datum, Uhrzeit, Name des Abrufenden, Grund der Abfrage und die E-Mail-Adresse des Benutzers erfasst werden. Eine Auswertung dieser Protokolle erfolgt stichprobenartig zur Kontrolle der Rechtmäßigkeit der Abfrage und bei vermuteten Sicherheitsverletzungen. Die Protokolldaten werden ein halbes Jahr aufbewahrt und anschließend gelöscht.

Die Bayerische Vermessungsverwaltung beabsichtigt, dieses Verfahren auf weitere Landratsämter und Gemeinden auszuweiten.

17.3.6 Security@School

Im Rahmen der Prüfungs- und Kontrolltätigkeit besuchte ich auch eine Schule, die an dem Programm „Security@School“ der Deutschen Telekom AG teilnimmt. Um den Anschluss der Netzwerke einer Schule sicherer zu machen, wird die Schule über eine von der Deutschen Telekom AG gelieferte Firewall mit Proxy-Diensten entweder über T-DSL/T-Online oder ISDN/T-Online an das Internet angeschlossen.

Die Firewall besitzt drei Netzwerkkarten und eine ISDN Karte, sodass über eine Netzwerkkarte oder die ISDN Karte der Zugang zum Internet und über die beiden verbleibenden Netzwerkkarten je das Schüler- und das Lehrer-/Verwaltungsnetzwerk angeschlossen werden können. Als Betriebssystem kommt ein vorkonfiguriertes GNU/Linux zum Einsatz.

Die Firewall setzt interne Netzwerkadressen auf eine offizielle Internet-Netzwerkadresse um (NAT, Native Adress Translation) und blockiert alle Zugriffe aus dem Internet auf interne Rechner. Es ist mit dieser Lösung somit nicht möglich, eigene Serverdienste (Web-Server) innerhalb der Schule zu betreiben. Es kann aber der Web-Server von T-Online verwendet werden, um einen Internetauftritt der Schule zu realisieren.

Zwischen den beiden internen Netzwerken ist ebenfalls keine Verbindung möglich, sodass das Lehrer-/Verwaltungsnetzwerk vom Schülernetzwerk und damit von möglichen, von dort ausgehenden Angriffsversuchen abgeschottet ist.

Das Lehrer-/Verwaltungsnetzwerk kann über NAT transparent auf alle Internetdienste zugreifen. Um die Geschwindigkeit zu steigern, steht zusätzlich noch ein WWW Proxy zur Verfügung, der für das Lehrer-/Verwaltungsnetzwerk keine Inhaltsfilterung vornimmt.

Für das Schülernetzwerk werden nur spezielle Internetdienste (http, https und ftp) über den auf der Firewall laufenden Proxy „squid“ zugelassen. Ein Routing der Schüler-Netzwerkadressen ins Internet erfolgt nicht (kein NAT). Da alle Seitenaufrufe aus dem Schülernetzwerk über den Proxy gehen müssen, kann dieser zur Filterung von Internetinhalten verwendet werden. Es gibt eine von der Telekom betreute Liste an gesperrten Seiten, die auf Anfrage der Schule ergänzt werden kann. Die Schule kann aber auch eine eigene Sperrliste generieren und pflegen. Die Sperrung von Seiten soll dazu dienen, Schülern keinen Zugriff auf jugendgefährdende Inhalte des Internets zu gewähren. Dies kann aber natürlich kein perfekter Schutz sein - es bleibt somit bei der Verantwortung der Lehrer, die Internetnutzung der Schüler sinnvoll zu begleiten.

Die Struktur und Realisierung dieser Lösung schätze ich als grundsätzlich gut ein, es kann aber nur ein Teil eines Sicherheitskonzeptes einer Schule für den Internetanschluss sein.

Auf alle Fälle müssen sowohl alle Rechnersysteme im Lehrer-/Verwaltungsnetzwerk als auch im Schülernetzwerk mit immer aktualisierter Virenschutzsoftware ausgestattet sein. Die Firewall kann nicht verhindern, dass virenverseuchte Daten und Programme aus dem Internet oder über Datenträger in das Netz gelangen. Diese Virenschutzsoftware darf auch nicht einfach von Anwendern deaktivierbar sein.

Auch wenn die Firewall gegen Angriffe aus dem Internet schützen kann, so müssen auf Rechnern, auf denen schutzwürdige Daten gespeichert sind, zusätzliche Sicherheitsmassnahmen getroffen werden. Am besten ist es sicherlich, wenn solche Rechner keinen Zugang zum Internet erhalten. Falls derartige Rechner als Bestandteil des Lehrer-/Verwaltungsnetzwerkes doch über die Firewall an das Internet angeschlossen werden, so werden sie zwar gegen Angriffe aus dem Internet und aus dem Schülernetzwerk geschützt, im Falle einer Fernwartung der Firewall, die auch unbemerkt durchgeführt werden kann, sind diese Rechner jedoch ungeschützt. Deshalb

muss hier besonders darauf geachtet werden, dass insbesondere auf diesen Rechnern aktuelle Sicherheitsupdates installiert sind, ein ausreichender Passwortschutz eingehalten wird und keine Freigaben für Zugriffe über das Netzwerk etc. eingerichtet sind. Sinnvollerweise sollte zusätzlich eine Verschlüsselung auf Datei-, Verzeichnis- oder Laufwerksebene durchgeführt werden.

Aus datenschutzrechtlicher Sicht bedenklich ist der verwendete Proxy. Dieser filtert alle Seitenaufrufe und kann somit genaue Auskunft über das Surfverhalten der Schüler geben. Die mitgelieferte Software zur Auswertung der Proxy-Logdateien „Calamaris“ erstellt eine Übersicht über die Verwendung des Proxy. Hieraus sind jedoch keine Rückschlüsse auf einzelne Rechner oder Personen möglich. Trotzdem wäre dies vermutlich bei einer detaillierteren Auswertung der Logdateien, auf die auch der Fernwartungsdienst zugreifen kann, problemlos möglich. Deshalb sollte der Proxy so konfiguriert sein, dass nicht die vollständige IP Adresse des Absenders in den Logdateien mitprotokolliert wird (etwa durch das Setzen des Parameters „client_netmask“ auf „255.255.255.0“ in der Konfigurationsdatei des Proxys squid, wodurch das letztes Segment der IP Adresse des Absenders immer durch „0“ ersetzt und somit anonymisiert wird). Ich habe dies der Schule so empfohlen; deren Stellungnahme steht noch aus.

Zusätzlich zu einer Firewall für die Internetanbindung empfiehlt es sich auch, auf den Rechnern des Schülernetzwerkes Software einzusetzen, die die Funktionalität der Rechner einschränkt. So sollten Schüler keine Software installieren oder ändern dürfen und nur die Software starten dürfen, die für Unterrichtszwecke nötig ist. Die von meinen Mitarbeitern besuchte Schule setzte dafür die Softwareprodukte „INIS Classic“ und „HDGuard“ ein. Damit lässt sich für bestimmte Klassen eine bestimmte Softwareauswahl festlegen, die der Lehrer freigeben kann. Ebenso werden dadurch die Rechner nach Gebrauch wieder in den Originalzustand versetzt, sodass keine persönlichen Daten auf den Rechnern verbleiben (Cookies etc.). Außerdem wird dadurch zusätzlich zur Antivirensoftware ein weiterer Schutz gegen Schadenssoftware installiert.

17.3.7 WLAN

Mittels eines WLANs (wireless local area network – lokales Rechnernetz über Funk) lassen sich Rechner ohne die Verwendung von Netzwerkkabeln vernetzen. Die WLAN Technologie eignet sich zur Erweiterung fest verdrahteter LANs und ermöglicht größere Mobilität. Dies hat zum Beispiel Vorteile in denkmalgeschützten Gebäuden, in denen die Verlegung von Kabeln nur

schwierig möglich ist, oder wenn die Teilnehmer des Rechnernetzes nicht immer an festen Arbeitsplätzen arbeiten (zum Beispiel Ärzte mit Laptops in Kliniken).

Standards

Ein minimales WLAN besteht aus zwei Rechnern mit WLAN-Karten, die im Ad-hoc-Modus betrieben werden. Diese beiden Rechner können ohne weitere Infrastruktur ein Netzwerk bilden und beispielsweise Dateien austauschen. Wird ein spezieller Empfänger und Sender benutzt, um mit den Endgeräten mit WLAN-Karten zu kommunizieren, spricht man vom Infrastruktur-Modus, der mit einer GSM-Zelle beim Mobilfunk verglichen werden kann.

Standardisiert ist die Übertragung mittels eines WLANs durch die IEEE 802.11 Working Group for Wireless Local Area Networks, die in den Standards IEEE 802.11 (bis 2Mbit/s), dem zurzeit am häufigst verwendeten IEEE 802.11b (bis 11Mbit/s) und IEEE 802.11a/g (bis 54Mbit/s) die technischen Voraussetzungen definiert hat. In diesen Standards werden die OSI-Schichten 1 (Physical Layer) und 2 (MAC-Layer) für WLANs spezifiziert. Die Funk-Übertragung findet im frei verfügbaren 2,4 GHz Band (Industrial Scientific Medical (ISM-) Band), das beispielsweise auch Bluetooth oder schnurlose DECT Telefone benutzen, oder im 5GHz Band statt.

Die maximale Sendeleistung einer Station ist in Europa auf 100mW beschränkt, womit sich innerhalb eines Hauses bis zu 150 Meter, außerhalb bis zu 500 Meter (bei eventuell nicht voller Übertragungsgeschwindigkeit) überbrücken lassen.

Geregelt wurde der Betrieb eines WLANs mit der Verfügung 122 im Amtsblatt 14/1997 (Vfg 122/1997) des damaligen Bundesministeriums für Post und Telekommunikation (BMPT) für den Betrieb von drahtlosen Datenfunkanlagen ab dem 21. Mai 1997. Mit dem Amtsblatt 22/1999 der Regulierungsbehörde für Telekommunikation und Post (RegTP) wurden mittels der Verfügung 154/1999 die bislang vorläufige Allgemeinzuteilung von Frequenzen nach Verfügung 122 in einigen Details präzisiert.

Innerhalb der eigenen Grundstücksgrenzen ist eine Nutzung ohne eine Anmeldung erlaubt. Bei dem Betrieb einer Richtfunkstrecke über die Grundstücksgrenzen hinaus muss diese bei der RegTP schriftlich angemeldet werden. Wird das WLAN einer nicht geschlossenen Benutzergruppe geöffnet, so ist dies eine lizenzpflichtige Nutzung, die eine Lizenz der Klasse 3 nach § 6

TKG erfordert und es werden dadurch entsprechende Gebühren laut Telekommunikationslizenzgebührenverordnung (TKLGebV) fällig.

Sicherheit

Soll ein WLAN zur Übertragung von schutzwürdigen Daten benutzt werden, so muss das WLAN, wie alle anderen Komponenten eines Rechnernetzes auch, in ein EDV Sicherheitskonzept eingegliedert werden. Problematisch bei WLANs ist, dass der physikalische Zugang zum Übertragungsmedium in der Regel unbemerkt, eventuell sogar ohne Betreten des Grundstücks des Betreibers, möglich ist. Somit kann nicht schon das Abschließen oder Deaktivieren von Netzwerksteckdosen als Zugangserschwernis dienen.

Damit ein Client mit einem so genannten Access Point (Empfangsstation, die den Zugang zum Netz ermöglicht) kommunizieren kann, muss auf beiden die gleiche Server Set ID (SSID) als Netzwerkname eingetragen sein. Die meisten heute verfügbaren Produkte werden mit Standardnamen ausgeliefert - diese sind bei Inbetriebnahme auf alle Fälle zu ändern. Einige Produkte erlauben es auch, als Netzwerkname „any“ anzugeben. Häufig ist dies sogar die Standardeinstellung. Das Geheimhalten des Netznamens ist nicht ausreichend, um einen Zugangsschutz gegenüber Unberechtigten zu gewährleisten, vor allem, da die SSID auch bei eingeschalteter Verschlüsselung im Klartext übertragen wird und somit leicht abgehört werden kann.

Des Weiteren kann der Zugang nur für bestimmte MAC Adressen erlaubt werden. Allerdings gibt es Möglichkeiten, die MAC Adresse einer WLAN Karte zu verändern, sodass eine Fälschung und damit ebenfalls ein unerlaubter Zugriff machbar ist.

Um ein Funknetz aufzufinden, gibt es inzwischen einfach zu bedienende Software. Da das so genannte „Wardriving“ (Auffinden von WLANs durch Umherfahren mit Auto und Laptop) und „Warchalking“ (Markieren von Empfangsbereichen von offenen oder geschlossenen WLANs mittels Kreidezeichen auf Wänden und Strassen) sich steigender Beliebtheit erfreut, kann nicht davon ausgegangen werden, dass ein ungesichertes WLAN lange unentdeckt bleibt.

Um die Sicherheit zu erhöhen, gibt es spezielle WLAN Verschlüsselungsverfahren, die zum einen den Zugang zu einem Access Point sperren können und zum anderen die Verbindung abhörsicherer machen können. Das hierfür meistens verwendete WEP (Wired Eqivalent Privacy) Pro-

tokoll erschwert den Zugriff. In der Vergangenheit wurden aber bereits einige Lücken und Schwächen bekannt und ausgenutzt. Die Verschlüsselung kann mit 40 Bit oder 128 Bit erfolgen. Es gibt Bestrebungen, den WEP Standard zum Beispiel mittels RC4 Fast Packet Keyring (IEEE 802.11i) sicherer zu machen, es bleibt aber abzuwarten, wie schnell sich ein sichereres WEP Protokoll durchsetzen wird.

Aufgrund der oben genannten Sicherheitsrisiken auf der Netzwerk-Transportebene müssen für ein Funknetz neben

- geheimen Netzwerknamen,
- restriktiver MAC Authentifizierung und
- WEP Verschlüsselung

zusätzliche Sicherheitsmassnahmen getroffen werden. Dabei handelt es sich um folgende:

- Trennung des WLAN Segments mittels einer Firewall vom internen, schützenswerten Netz
- Unterbindung einer direkten Zugriffsmöglichkeit auf die internen Netzwerkkomponenten aus dem WLAN-Segment heraus
- Verschlüsselung der im WLAN genutzten Dienste (etwa Verwendung von https statt http) oder Schutz des gesamten Netzwerkverkehrs mittels eines VPN (Virtual Private Network)
- Ggf. Einsatz von Verschlüsselung auf Anwendungsebene

Somit gelten für die Datenübermittlung von mobilen Rechner aus ähnliche Sicherheitsanforderungen, wie bei Rechnern, die über das Internet auf das interne Netz zugreifen können sollen.

Des Weiteren müssen auch die mobilen Rechner selbst möglichst gut gegen Angriffe geschützt werden, denn sie befinden sich keineswegs hinter einer sicheren Firewall, sondern zusammen mit einem potenziellen Angreifer außerhalb der Firewall. Auch das Abhandenkommen (Diebstahl) eines WLAN Clients (Laptop) birgt die Gefahr, dass nicht nur die auf dem Laptop gespeicherten Daten in unberechtigte Hände gelangen, sondern unter Umständen ein Unbefugter mittels der registrierten WLAN Karte und richtiger SSID auf das interne Netz zugreifen kann. Deshalb sind die Nutzer darauf zu sensibilisieren, besonders auf diese Geräte zu achten und einen Verlust der WLAN Karte sofort zu melden. Die Geräte selbst sind mit wirksamen Zugriffssicherungsmechanismen auszustatten.

Leider liefern die meisten Hersteller ihre Produkte mit den minimalsten Sicherheitseinstellungen als Standard aus, sodass zwar sehr einfach eine erste Inbetriebnahme eines WLAN Segments erfolgen kann, dieses danach aber offen für vielerlei Angriffe ist. Es liegt am Betreiber, alle bekannten Sicherheitslücken durch geeignete Maßnahmen zu schließen und den Schaden durch eventuell neue Angriffsmethoden möglichst gering zu halten.

17.3.8 Persönlichkeitsschutz im Sozialamt

Gemäß § 35 Abs. 1 Satz 1 Sozialgesetzbuch (SGB) I haben Hilfe Suchende Anspruch darauf, dass die sie betreffenden Sozialdaten (§ 67 Abs. 1 SGB X) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis). Der Sozialleistungsträger ist damit verpflichtet, u. a. durch technische und organisatorische Maßnahmen (vgl. § 78 a SGB X) zu gewährleisten, dass Sozialdaten der Antragsteller bzw. Leistungsbezieher niemandem unberechtigterweise zur Kenntnis gelangen können.

Diese Verpflichtung folgt aus dem Grundrecht auf informationelle Selbstbestimmung. Neben diesem Grundrecht des Antragstellers steht allerdings ein ebenfalls grundgesetzlich garantiertes Recht auf körperliche Unversehrtheit der Bediensteten der jeweiligen Sozialbehörde. Insbesondere wenn der Antragsteller seine Belange nicht zu seiner Zufriedenheit berücksichtigt oder gewürdigt findet, kann es in Sozialbehörden auch zu verbalen oder gar körperlichen Attacken gegen die dortigen Bediensteten kommen. Manche Sozialämter sehen in dem Offenstehenlassen von Zwischen- und Verbindungstüren den bestmöglichen Schutz vor solchen Angriffen, da es die Möglichkeit bietet, der oder dem Angegriffenen zu Hilfe zu kommen. Im 15. Tätigkeitsbericht wurde diese Maßnahme als Lösungsmöglichkeit angesehen.

Neuerliche Beschwerden über das Offenlassen der Türen haben mich veranlasst, diese Frage erneut zu überprüfen. Ich habe zunächst versucht die widerstreitenden Interessen dadurch einer Lösung zuzuführen, dass ich die betreffenden Sozialämter aufgefordert habe, grundsätzlich den Antragsteller zu Beginn des Gespräches zu fragen, ob er mit dem Offenstehen der Türe einverstanden ist. Bei geöffneten Türen müsse darauf geachtet werden, dass die Besprechung zwischen einem Antragsteller und dem Sozialamtsbediensteten in einer Lautstärke geführt wird, dass die Inhalte der Besprechung im Nebenzimmer nicht zu verstehen sind.

Das Offenhalten der Verbindungstüren müsse die Ausnahme für Bedrohungen oder sonstige Agressionen bleiben, wobei bei der Entscheidung über die Verfahrensweise auf die vom Bediensteten subjektiv empfundene Bedrohungssituation abgestellt werden könne, da mögliche Angriffshandlungen unter Umständen nicht vorausgesehen werden könnten.

Vorstehender Lösungsversuch ist allerdings nicht das Optimum, insbesondere wenn man berücksichtigt, dass bei Antragstellern, von denen Agressionen nicht zu befürchten sind, eigentlich auch kein Anlass besteht, nach dem Einverständnis für das Offenhalten der Türen zu fragen und im umgekehrten Fall es auf sein Einverständnis nicht ankommen kann, wenn in dem Offenstehenlassen der Türe die gebotene Sicherheitsmaßnahme gesehen werden kann.

Bessere Lösungen sind deshalb zu prüfen. Dabei ist zu berücksichtigen, dass eine Gefährdung bzw. Beeinträchtigung des Rechts auf informationelle Selbstbestimmung unverhältnismäßig ist, wenn es zumutbare Alternativen gibt, den Schutz der Bediensteten anderweitig ebenso effektiv zu gewährleisten. Eine solche Alternative zum Offenstehenlassen der Türe sehe ich in einer Alarmeinrichtung, vergleichbar einem Alarmknopf bei Banken, die bei Betätigung in den Nachbarzimmern ein akustisches Signal auslöst und so eine schnelle Hilfeleistung im Bedarfsfall ermöglicht. Auch diese Maßnahme wurde im 15. Tätigkeitsbericht als Lösungsmöglichkeit angesehen. Ich habe deshalb die betreffende Kommune dringend gebeten, den Einbau einer Alarmanlage zu prüfen, oder mir zwingende Hinderungsgründe darzulegen.

Mit wurde entgegen gehalten, dass das Offenstehenlassen der Türen für das Sicherheitsgefühl der meist jungen Bediensteten des Sozialamts erforderlich sei. Ich nehme diesen Einwand ernst. Ich habe allerdings große Zweifel, ob offene Türen tatsächlich in einer Weise zu einer solchen Erhöhung des Sicherheitszustandes beitragen würden, die die Gefahr des Bruchs des Sozialgeheimnisses rechtfertigen würde. Ich bin gleichwohl der Auffassung, dass Sozialdatenschutz primär durch Einbau einer Alarmanlage gewährleistet werden muss. Das Sicherheitsgefühl der Bediensteten kann durch praktische Erprobung der Alarmanlage gefördert werden. In diesem Sinn bin ich nochmals an die betreffende Kommune herangetreten.

17.4 Orientierungshilfen

Im Berichtszeitraum hat meine Geschäftsstelle folgende Orientierungshilfen überarbeitet:

- „Grundsätze für „Benutzerrichtlinien für den Umgang mit Internet““ (http://www.datenschutz-bayern.de/technik/orient/ibenrili.pdf)

- „Einrichtung eines Benutzerservices“ (http://www.datenschutz-bayern.de/technik/orient/benserv.pdf)

- „Aufgaben eines behördlichen Datenschutzbeauftragten“ (http://www.datenschutz-bayern.de/technik/orient/bdsb.pdf) und

- „Verfahrensverzeichnis“ auch mit dem neuen Titel „Verfahrensbeschreibung“ http://www.datenschutz-bayern.de/download/Verfahrensbeschreibung.zip versehen.

Diese Orientierungshilfen können unter den o.a. URL direkt von meiner Home-Page und auch unter der Rubrik „Technik“ abgerufen werden.

Aufgrund Gesetzesänderung ist das Führen eines Anlagenverzeichnisses nicht mehr erforderlich (vgl. Abschnitt 17.1.6, „Novelliertes Bayerisches Datenschutzgesetz“), sodass die Mustervorlage „Anlagenverzeichnis“ entbehrlich und daher entfernt wurde.

Auf die Orientierungshilfe „Tele- und Mediendienste“ mit Stand 01. Juli 2002 meines Hamburger Kollegen „http://fhh.hamburg.de/coremedia/generator/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/veroeffentlichungen/informationsmaterialien/internet/orientierungshilfe-tele-und-mediendienste.html“ darf ich hier zusätzlich verweisen.

18 Die Datenschutzkommission

Mit In-Kraft-Treten der Änderung des Bayerischen Datenschutzgesetzes zum 01.12.2000 wurde beim Landtag eine Datenschutzkommission gebildet, die an die Stelle des bisherigen Beirats trat und ohne Änderung dessen Aufgabe, die Unterstützung des Landesbeauftragten für den Datenschutz in seiner Arbeit, übernahm. 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 aber 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 bestellt. 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 Datenschutzgesetzes wahr. Für ihre Bestellung und Amtszeit gelten die bisherigen Vorschriften.

Der Datenschutzkommission beim Landtag 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	Bärbel Narnhammer	SPD
Franz Schindler	SPD	Joachim Wahnschaffe	SPD
Christine Stahl	BÜNDNIS90/ DIE GRÜNEN	Susanna Tausendfreund	BÜNDNIS90/ DIE GRÜNEN

ab 15.02.2002:

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	Joachim Wahnschaffe	SPD
Bärbel Narnhammer	SPD	Franz Schindler	SPD
Christine Stahl	BÜNDNIS90/ DIE GRÜNEN	Susanna Tausendfreund	BÜNDNIS90/ DIE GRÜNEN

ab 14.05.2002:

Franz Brosch	CSU	Prof. Dr. Hans Gerhard Stockinger	CSU
Petra Guttenberger	CSU	Johann Neumeier	CSU
Alexander König	CSU	Christian Meißner	CSU
Manfred Weber	CSU	Thomas Obermeier	CSU
Bärbel Narnhammer	SPD	Franz Schindler	SPD
Dr. Klaus Hahnzog	SPD	Joachim Wahnschaffe	SPD
Christine Stahl	BÜNDNIS90/ DIE GRÜNEN	Susanna Tausendfreund	BÜNDNIS90/ DIE GRÜNEN

Für die **Staatsregierung**:

Christian P. Wilde	Bayerisches Staatsministerium des Innern	Hubert Kranz	Bayerisches Staatsministeri-um der Finanzen

Für die **Sozialversicherungsträger**:

Werner Krempl	Erster Direktor der LVA Oberfranken und Mittelfranken	Dr. Helmut Platzer	Vorstandsvorsit-zender der AOK Bayern

Für die **Kommunalen Spitzenverbände**:

Klaus Eichhorn	Geschäftsführen-der 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	Bildender Künstler Präsidiumsmit-glied des Ver-bandes Freier Berufe in Bayern Vorsitzender des BBK München und Oberbayern e. V. Berufsver-band Bildender Künstler e.V.

Den Vorsitz in der Kommission führt Franz Brosch, MdL. Sein Stellvertreter bis zum 19.03.2001 war Dr. Klaus Hahnzog, MdL; Stellvertreterin seit dem 20.03.2001 ist Bärbel Narnhammer, MdL.

Die Datenschutzkommission tagte im vergangenen Berichtszeitraum 10 Mal. Dabei befasste sie sich u. a. mit folgenden Themen:

- Beratung des 20. Tätigkeitsberichts
- Berichte von Datenschutzkonferenzen
- Datenschutz und Innere Sicherheit nach dem 11. September 2001
- Videoüberwachung
- Virtueller Marktplatz Bayern
- Entwürfe verschiedener Landtagsfraktionen für ein Bayerisches Informationsfreiheitsgesetz
- Datenerhebungen durch überörtliche Sozialhilfeträger über behinderte Menschen, insbesondere zur Erstellung eines Gesamtplans gemäß § 46 BSHG
- Datenschutz bei der Behandlung chronisch kranker Menschen im Rahmen der „Disease-Management-Programme“ (DMPe) der gesetzlichen Krankenkassen nach § 137 f SGB V.

Anlage 1: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2001: Novellierung des G 10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,

- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und

- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

- Alle Neuregelungen wie z.B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

- Dem BND wird nicht mehr nur die „strategische Überwachung“ des nicht-leitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischen Überwachung“ nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 2: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2001: Datenschutz beim elektronischen Geschäftsverkehr

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 136/01) vorliegen. Danach sollen Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Darüber hinaus sollen die Anbieterinnen und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden.

Die Datenschutzbeauftragten weisen darauf hin, dass sich anhand dieser Daten nachvollziehen lässt, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen nachgeht. Eine pauschale Registrierung jeder Inanspruchnahme von Telediensten zur staatlichen Überwachung greift tief in das Persönlichkeitsrecht der betroffenen Nutzerinnen und Nutzer ein und berührt auf empfindliche Weise deren Informationsfreiheit. Der Bundesrat wird daher aufgefordert, diese Anträge abzulehnen.

Anlage 3: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2001: Novellierung des Melderechtsrahmengesetzes

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf - wie in seiner Begründung ausdrücklich betont wird - nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

Anlage 4: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2001: Informationszugangsgesetze

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegen steht, wenn die Privatssphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung ent-

sprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

Anlage 5: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2001: Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

Anlage 6: Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.03.2001: Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden

muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,

- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,

- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,

- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

Anlage 7: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12.03.2001: Anlasslose DNA-Analyse aller Männer verfassungswidrig

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den „genetischen Fingerabdruck“ aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potentielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anlage 8: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24.04.2001: Veröffentlichung von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der

beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 09.03.1988 - 1 BvL 49/86 - zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z.B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

Anlage 9: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10.05.2001: Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße „Surfen“ zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Tele-

dienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

Anlage 10: Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 01.10.2001 zur Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z.B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des

Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anlage 11: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26.10.2001: Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als **Pflichtkarte**. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der

Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (**Grundsatz der Freiwilligkeit**).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,

- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,

- welche ihrer Daten auf der Karte wieder gelöscht werden,

- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und

- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem „Arzneimittelpass“ keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den „Arzneimittelpass“ auf der **Krankenversichertenkarte** gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offenlegen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z.B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anlage 12: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001 zur gesetzlichen Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;

- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;

- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;

- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;

- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;

- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;

- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;

- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;

- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;

- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;

- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage zu der Entschließung zur gesetzlichen Regelung von genetischen Untersuchungen

Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Allgemeines

Gegenstand

Zu regeln ist die Zulässigkeit genetischer Untersuchungen beim Menschen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten. Neben allgemeinen Regelungen sind besondere Bestimmungen zu genetischen Untersuchungen

1. zu medizinischen Zwecken

2. im Zusammenhang mit Arbeits- und Versicherungsverhältnissen

3. zur Abstammungsklärung und Identifizierung außerhalb der Strafverfolgung

4. zu Forschungszwecken

zu treffen.

Ziel, Benachteiligungsverbot

(1) Ziel der Regelungen ist der Schutz der Menschenwürde, der Persönlichkeit und der informationellen Selbstbestimmung der Betroffenen bei genetischen Untersuchungen.

(2) Niemand darf wegen seiner Erbanlagen oder wegen der Weigerung, eine genetische Untersuchung bei sich durchführen zu lassen, benachteiligt werden.

Begriffe

1. **Genetische Untersuchungen:** Untersuchungen auf Chromosomen-, Genprodukt- oder molekularer DNS / RNS-Ebene, die darauf abzielen, Informationen über das Erbgut zu erhalten;

2. **Prädiktive Untersuchungen:** vor- oder nachgeburtliche genetische Untersuchungen mit dem Ziel, Erbanlagen einer Person, insbesondere Krankheitsanlagen vor dem Auftreten von Symptomen oder einen Überträgerstatus, zu erkennen;

3. **Überträgerstatus:** Erbablagen, die erst in Verbindung mit entsprechenden Erbanlagen eines Partners oder einer Partnerin eine Krankheitsanlage bei den gemeinsamen Nachkommen ausbilden;

4. **Pränatale Untersuchungen:** vorgeburtliche genetische Untersuchungen mit dem Ziel, während der Schwangerschaft Informationen über das Erbgut des Embryos oder des Fötus zu gewinnen;

5. **Reihenuntersuchung:** genetische Untersuchungen, die systematisch der gesamten Bevölkerung oder bestimmten Gruppen der Bevölkerung angeboten werden, ohne dass bei den Betroffenen Anhaltspunkte dafür bestehen, dass die gesuchten Erbanlagen bei ihnen vorhanden sind;

6. **Diagnostische genetische Untersuchungen:** genetische Untersuchungen zur Abklärung der Diagnose einer manifesten Erkrankung oder zur Vorbereitung oder Verlaufskontrolle einer Behandlung;

7. **Probe:** die für eine genetische Untersuchung vorgesehene oder genutzte biologische Substanz;

8. **Genetische Daten:** im Zusammenhang mit genetischen Untersuchungen erlangte Informationen über eine Person;

9. **Betroffene Person:** die Person, von der eine Probe vorliegt oder deren genetische Daten erhoben, verarbeitet oder genutzt werden; bei pränatalen Untersuchungen auch die schwangere Frau;

10. **Verarbeiten:** das Speichern, Verändern, Übermitteln, Sperren und Löschen erhobener personenbezogener genetischer Daten.

Zulässigkeit genetischer Untersuchungen

Genetische Untersuchungen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten bedürfen der freiwilligen, schriftlichen Einwilligung der betroffenen Person nach Aufklärung. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen zu regelnden und in der Strafprozessordnung geregelten Ausnahmen.

Zulassung zur Durchführung genetischer Untersuchungen

(1) Wer genetische Untersuchungen durchführen will, bedarf hierfür der Zulassung durch die zuständige Aufsichtsbehörde des Landes.

(2) Die Zulassung wird erteilt, wenn Gewähr dafür besteht, dass

- die Untersuchungen und ihre Auswertungen sorgfältig und nach dem Stand von Wissenschaft und Technik durchgeführt werden,

- die Regelungen gemäß diesen Vorschlägen eingehalten, insbesondere Information und Beratung der betroffenen Person und die Datensicherheit gewährleistet werden und

- in der antragstellenden Person die berufsrechtlichen und gewerberechtlichen Voraussetzungen vorliegen.

(3) Das Nähere regelt die Bundesregierung durch Rechtsverordnung.

Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen

Genetische Testverfahren dürfen nur für den Gebrauch durch Ärztinnen, Ärzte oder Labors eingeführt oder in Verkehr gebracht werden. Das öffentliche Angebot, genetische Untersuchungen zu medizinischen Zwecken ohne individuelle Beratung der betroffenen Person durchzuführen, ist unzulässig. Die Berufsfreiheit, Artikel 12 Absatz 1 Satz 2 Grundgesetz, wird insoweit eingeschränkt.

Zweckbindung

Die für die genetische Untersuchung vorgesehene oder genutzte Probe und die genetischen Daten dürfen nur für den Zweck verwandt und für die Dauer aufbewahrt werden, zu denen die betroffene Person ihre Einwilligung erklärt hat oder zu denen ein Gericht oder eine Verwaltungsbehörde eine Anordnung getroffen hat. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen geregelten Ausnahmen.

Datensicherheit

(1) Proben und genetische Daten sind vor dem Zugriff unbefugter Dritter wirksam zu schützen. Dies gilt auch in Bezug auf Mitarbeiterinnen und Mitarbeiter der untersuchenden und datenverarbeitenden Stelle, die an der genetischen Untersuchung, Aufklärung und Beratung nicht beteiligt sind oder waren.

(2) Genetische Daten sind von anderen Datenarten gesondert zu speichern.

(3) Im Übrigen gilt hinsichtlich der genetischen Daten die Bestimmung des Bundesdatenschutzgesetzes über die technischen und organisatorischen Maßnahmen der Datensicherheit in der jeweils geltenden Fassung.

Einsichts- und Auskunftsrecht

Die betroffene Person hat das Recht, unentgeltlich Einsicht in die Dokumentationen zur genetischen Untersuchung einschließlich Aufklärung und Beratung zu nehmen und Auskunft über die zu ihr gespeicherten Daten zu verlangen.

Genetische Untersuchungen zu medizinischen Zwecken

Grundsatz

(1) Zu medizinischen Zwecken dürfen prädiktive Untersuchungen nur durchgeführt werden, wenn sie nach ärztlicher Indikation der Vorsorge, der Behandlung oder der Familienplanung der betroffenen Person dienen.

(2) Eine genetische Untersuchung zum Erkennen eines Überträgerstatus ist nur zu Zwecken der konkreten Familienplanung zulässig.

(3) Für diagnostische genetische Untersuchungen gelten nur die Anforderungen gemäß dem Arztvorbehalt (siehe unten) und an diagnostische genetische Untersuchungen bei behinderten Personen (siehe am Ende dieses Abschnitts).

Pränatale Untersuchungen

Pränatale Untersuchungen sind auf das Erkennen solcher Krankheiten zu richten, die vorgeburtlich behandelt werden können. Für darüber hinausgehende genetische Untersuchungen gelten die Richtlinien der Bundesärztekammer zur pränatalen Diagnostik. Das Geschlecht darf gezielt nur zu medizinischen Zwecken festgestellt werden.

Ob darüber hinaus auch schwere Behinderungen und Anlagen für schwere, nicht behandelbare Krankheiten Ziele pränataler DNA-Untersuchungen sein dürfen, muss der gesellschaftspoliti-

schen Diskussion, der fachmedizinischen Bewertung und der Verantwortung des Gesetzgebers überlassen bleiben.

Genetische Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen

(1) Genetische Untersuchungen bei Minderjährigen sind nur zulässig, wenn ihre Durchführung vor Erreichen der Volljährigkeit erforderlich ist, um den Ausbruch einer Krankheit zu vermeiden oder zu verzögern, eine Heilung oder Verlaufsmilderung zu erreichen oder spätere besonders belastende Untersuchungen zu vermeiden. Bei Aufklärung, Beratung und Einwilligung (siehe unten) ist die Einsichtsfähigkeit der betroffenen minderjährigen Person zu berücksichtigen.

(2) Prädiktive Untersuchungen bei nicht einsichtsfähigen Erwachsenen dürfen sich nur auf das Erkennen von Krankheiten richten, deren Ausbruch vermieden oder verzögert oder bei denen eine Heilung oder Verlaufsmilderung erreicht werden kann. Die Einwilligung obliegt dem gesetzlichen Vertreter.

Reihenuntersuchungen

(1) Genetische Reihenuntersuchungen bedürfen der Zulassung durch die zuständige Landesbehörde.

(2) Voraussetzung für die Zulassung ist, dass

- die Reihenuntersuchung gerichtet ist auf das Erkennen von verbreiteten oder schweren Krankheiten, die unverzüglich nach dem Untersuchungsergebnis behandelt werden können, oder von Krankheiten, deren Ausbruch verhindert werden kann,
- die Untersuchungsmethode eindeutige Ergebnisse liefert,
- die Freiwilligkeit der Teilnahme und die genetische Beratung gewährleistet und
- der Datenschutz gesichert ist.

Arztvorbehalt

(1) Prädiktive Untersuchungen dürfen nur von Fachärztinnen und Fachärzten für Humangenetik veranlasst werden. Diagnostische genetische Untersuchungen dürfen auch von anderen zur Berufsausübung zugelassenen Ärztinnen und Ärzten veranlasst werden.

(2) Die veranlassende Ärztin oder der veranlassende Arzt hat die Aufklärung und Beratung (siehe nachstehend) und die Einholung und Dokumentation der Einwilligung (siehe unten) sicherzustellen.

Aufklärung und Beratung

(1) Vor und nach einer prädiktiven genetischen Untersuchung ist die betroffene Person umfassend aufzuklären und zu beraten, um ihr eine selbstbestimmte Entscheidung gemäß den Anforderungen an die Einwilligung (siehe unten) zu ermöglichen.

(2) Die betroffene Person und gegebenenfalls ihr gesetzlicher Vertreter muss insbesondere aufgeklärt werden über

- Ziel, Art, Aussagekraft und Risiko der Untersuchung und die Folgen ihrer Unterlassung;
- mögliche, auch unerwartete Ergebnisse der Untersuchung;
- mögliche Folgen des Untersuchungsergebnisses, einschließlich physischer und psychischer Belastungen der betroffenen Person oder ihrer Familie;
- Behandlungsmöglichkeiten für die gesuchte Krankheit;
- den geplanten Umgang mit der Probe und den genetischen Daten einschließlich des Orts und der Dauer der Aufbewahrung bzw. Speicherung;
- die Einflussmöglichkeiten und Datenschutzrechte der betroffenen Person;

- weitere Beratungs- und Unterstützungsmöglichkeiten.

(3) Aufklärung und Beratung dürfen nur der individuellen und familiären Situation der betroffenen Person und den möglichen psychosozialen Auswirkungen des Untersuchungsergebnisses auf sie und ihre Familie Rechnung tragen.

(4) Bei Reihenuntersuchungen kann in begründeten Ausnahmefällen die Aufklärung in standardisierter Form erfolgen, wenn zugleich die Möglichkeit einer zusätzlichen individuellen Beratung angeboten wird.

(5) Bei pränatalen Untersuchungen ist der Partner der betroffenen Frau in die Beratung einzubeziehen, sofern die Frau einwilligt. Auf Stellen der Schwangerschaftskonfliktberatung ist hinzuweisen.

(6) Bei genetischen Untersuchungen zum Erkennen eines Überträgerstatus soll der Partner oder die Partnerin der betroffenen Person in die Aufklärung und Beratung einbezogen werden.

Einwilligung

(1) Nach der Aufklärung und Beratung entscheidet die betroffene Person nach angemessener Bedenkzeit in freier Selbstbestimmung darüber,

- ob die genetische Untersuchung durchgeführt werden soll,

- welches Ziel die genetische Untersuchung hat,

- ob sie auch unvermeidbare weitere Untersuchungsergebnisse zur Kenntnis nehmen will,

- wie gegebenenfalls mit der Probe und den genetischen Daten weiter verfahren werden soll.

Soweit die betroffene Person vom Ergebnis, auf das die Untersuchung zielt, keine Kenntnis

nehmen will, soll außer bei Reihenuntersuchungen grundsätzlich auf die genetische Untersuchung verzichtet werden.

(2) Die betroffene Person oder ihr gesetzlicher Vertreter hat die vorherige Aufklärung und Beratung schriftlich zu bestätigen und die Einwilligung in die genetische Untersuchung und in den vereinbarten Umgang mit der Probe und den genetischen Daten schriftlich zu erklären.

(3) Die Einwilligung kann widerrufen werden mit der Folge, dass noch nicht erfolgte Maßnahmen unterbleiben, schon vorliegende Proben vernichtet und die im Zusammenhang mit der Untersuchung erhobenen und gespeicherten Daten gelöscht werden.

Unterrichtung über das Untersuchungsergebnis

(1) Die veranlassende Ärztin oder der veranlassende Arzt teilt das Ergebnis der genetischen Untersuchung nur der betroffenen Person, bei Minderjährigen auch oder nur ihrem gesetzlichen Vertreter mit und berät über die möglichen Folgen und Entscheidungsalternativen.

(2) Ist das Ergebnis nach ärztlicher Erkenntnis auch für Verwandte der betroffenen Person von Bedeutung, hat die Ärztin oder der Arzt bei der nachgehenden Beratung der betroffenen Person auch auf das Recht der Verwandten hinzuweisen, ihre Erbanlagen nicht zur Kenntnis zu nehmen. Will die betroffene Person die Verwandten gleichwohl unterrichten, soll die Beratung auch die Möglichkeit umfassen, die Ärztin oder den Arzt mit der Unterrichtung von Verwandten der betroffenen Person zu beauftragen.

(3) Gegen den Willen der betroffenen Person oder ihres gesetzlichen Vertreters darf die veranlassende Ärztin oder der veranlassende Arzt Verwandte oder Partner der betroffenen Person nur dann von dem Untersuchungsergebnis unterrichten, wenn und soweit dies zur Wahrung erheblich überwiegender Interessen dieser Personen erforderlich ist.

Diagnostische genetische Untersuchung bei behinderten Personen

Bei diagnostischen genetischen Untersuchungen, die sich auf die Ursache einer Behinderung der betreffenden Person beziehen, gelten die Anforderungen an die Einwilligung und Unterrichtung über das Untersuchungsergebnis entsprechend.

Genetische Untersuchungen im Zusammenhangmit Arbeits- und Versicherungsverhältnissen

Grundsatz

Arbeitgebern und Versicherern ist es verboten, als Voraussetzung für einen Vertragsabschluss oder während des Vertragsverhältnisses prädiktive genetische Untersuchungen an betroffenen Arbeits- oder Versicherungsvertragsbewerbern oder Vertragspartnern durchzuführen oder zu veranlassen oder Ergebnisse von genetischen Untersuchungen zu verlangen, entgegenzunehmen oder sonst zu nutzen. Aus einer wahrheitswidrigen Beantwortung können Arbeitgeber oder Versicherer grundsätzlich keine Rechte ableiten (Ausnahmen siehe unten).

Arbeitsverhältnis

Bleibt der Arbeitsplatz trotz vorrangiger Arbeitsschutzmaßnahmen mit einer erhöhten Erkrankungs- oder Unfallgefahr verbunden, für deren Einritt nach dem Stand der Wissenschaft eine bestimmte Genstruktur der Betroffenen von Bedeutung ist, ist eine Arbeitsplatzbewerberin oder ein Arbeitsplatzbewerber hierauf hinzuweisen. Die Betriebsärztin oder der Betriebsarzt soll die betroffene Person hinsichtlich einer geeigneten genetischen Untersuchung beraten und ihr dafür zugelassene Ärztinnen oder Ärzte benennen.

Ausnahmen für das Versicherungsverhältnis

(1) Strebt die betroffene Person eine Versicherung mit einer Leistungssumme über 250.000 € an, ist der Versicherer berechtigt zu fragen, ob und gegebenenfalls wann bei der betroffenen Person eine prädiktive genetische Untersuchung durchgeführt wurde. Bei arglistigem Verschweigen kann der Versicherer den Versicherungsvertrag kündigen.

(2) Bestehen konkrete Anhaltspunkte, insbesondere aufgrund des Zeitabstandes zwischen genetischer Untersuchung und Versicherungsantrag, dafür, dass die Höhe der gewünschten Versicherungsleistung mit dem Ergebnis der genetischen Untersuchung zusammenhängt, kann der Versicherer das Ergebnis der genetischen Untersuchung verlangen. Dies gilt nicht für eine genetische Untersuchung, die bei der betroffenen Person pränatal oder während der Minderjährigkeit oder einer Einsichtsunfähigkeit durchgeführt wurde. In diesen Fällen darf der Versicherer das Ergebnis der genetischen Untersuchung von der betroffenen Person entgegennehmen.

Genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung

Grundsatz

(1) Zu Zwecken der Abstammungsklärung und der Identifizierung dürfen nur die dazu geeigneten und erforderlichen genetischen Untersuchungen (DNA-Identifizierungsmuster) durchgeführt werden. Diagnostische oder prädiktive Untersuchungen nach Krankheitsanlagen oder Merkmalen der betroffenen Person sind unzulässig. Abgesehen vom Merkmal Geschlecht sind unvermeidliche Überschussinformationen so früh wie möglich zu vernichten.

(2) Die untersuchende Stelle hat selbst die Proben bei der betroffenen Person zu entnehmen und dies zu dokumentieren.

(3) Die Proben sind zu vernichten, wenn die betroffene Person dies wünscht oder ein Gericht die Vernichtung anordnet, im Übrigen wenn die genetische Untersuchung durchgeführt ist. Die Dokumentation ist 10 Jahre aufzubewahren.

Einwilligung

Genetische Untersuchungen zu Zwecken der Abstammungsklärung oder Identifizierung dürfen nur mit schriftlicher Einwilligung der betroffenen Person oder ihres gesetzlichen Vertreters oder auf gerichtliche oder behördliche Anordnung durchgeführt werden. Für genetische Untersuchungen zur Abstammungsklärung bei Minderjährigen gilt § 1629 BGB.

Anordnung genetischer Untersuchungen zu Identifizierungszwecken

(1) In gerichtlichen und Verwaltungsverfahren kann das Gericht bzw. die Verwaltungsbehörde eine genetische Untersuchung zu Identifizierungszwecken anordnen, wenn die Identität einer Partei, eines Beteiligten oder einer für das Verfahren wichtigen dritten Person oder Leiche in Zweifel steht und nicht auf andere Weise geklärt werden kann. Ist die Identitätsfeststellung Voraussetzung für die Gewährung von behördlichen Genehmigungen oder Leistungen an die betroffene Person, ist die genetische Untersuchung nur mit ihrer Einwilligung zulässig.

(2) Die Anordnung hat die Art der Probe, das Ziel der Untersuchung sowie den Zeitpunkt der Vernichtung der Probe und der Löschung der genetischen Daten festzulegen. Bei lebenden Personen ist die Probe ohne Eingriff in die körperliche Unversehrtheit zu entnehmen, es sei denn, die betroffene Person willigt in einen Eingriff ein.

Genetische Untersuchungen zu Forschungszwecken

Konkrete, zeitlich befristete Forschungsvorhaben

(1) Für konkrete, zeitlich befristete Forschungsvorhaben ist die genetische Untersuchung von Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten zulässig, wenn

1. die Proben und die genetischen Daten der betroffenen Person nicht mehr zugeordnet werden können oder

2. im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert, die betroffene Person nach den Anforderungen für Forschungsvorhaben eingewilligt hat (siehe unten) oder

3. im Falle, dass weder auf die Zuordnungsmöglichkeit verzichtet, noch die Einwilligung eingeholt werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt

und der Forschungszweck nicht auf andere Weise zu erreichen ist.

(2) In den Fällen der Ziffer (1) Nr.2 und 3 sind bei Proben vor der Untersuchung, bei genetischen Daten vor der Verarbeitung oder Nutzung die Merkmale, mit denen ein Personenbezug hergestellt werden kann, gesondert zu speichern. Die Zuordnungsmöglichkeit ist aufzuheben, sobald der Forschungszweck es erlaubt und schutzwürdige Interessen der betroffenen Person gemäß der Regelung über deren Rechte (siehe unten) nicht entgegenstehen.

(3) Die Proben dürfen nur im Rahmen des Forschungsvorhabens untersucht, die genetischen Daten dürfen nur zu den Zwecken verarbeitet oder genutzt werden, für die sie im Rahmen des Forschungsvorhabens erhoben wurden.

(4) Mit Beendigung des Forschungsvorhabens sind die Proben zu vernichten und die genetischen Daten zu löschen. Ist ihre Aufbewahrung oder Speicherung zum Zwecke der Selbstkontrolle der Wissenschaft erforderlich, ist dies in pseudonymisierter Form für einen Zeitraum von längstens 10 Jahren zulässig.

(5) Konkrete, zeitlich befristete Forschungsvorhaben nach Ziffer(1) bedürfen der vorherigen Zustimmung der zuständigen Ethikkommission.

Sammlungen von Proben und genetischen Daten

(1) Das Sammeln von Proben einschließlich isolierter DNS oder RNS oder von genetischen Daten zu allgemeinen Forschungszwecken ist nur zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Entnahme der Probe sowie die Aufnahme von Probe und Daten in die Sammlung eingewilligt haben (siehe unten) Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben oder genetischer Daten.

(2) Die Zuordnung der Probe und der genetischen Daten zur betroffenen Person ist vor der Aufnahme in die Sammlung aufzuheben. Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.

(3) Vor einer Weitergabe von Proben und einer Übermittlung genetischer Daten für konkrete Forschungsvorhaben ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung gemäß den Regelungen bei Treuhändern (siehe unten) vorzunehmen.

(4) Der Träger einer Sammlung hat eine kontinuierliche interne Datenschutzkontrolle sicher zu stellen. Bei Trägerwechsel gehen alle Verpflichtungen aus diesem Gesetz auf den neuen Träger über. Soll eine Sammlung beendet werden, sind die Proben zu vernichten und die genetischen Daten sowie die beim Treuhänder (siehe unten) gespeicherten Daten zu löschen.

(5) Die Einrichtung einer neuen und die Übernahme einer bestehenden Sammlung nach Ziffer (1) bedürfen der Zustimmung durch die zuständige Ethikkommission. Die Einrichtung ist mit dem Votum der Ethikkommission und unter Darlegung der in den Vorschlägen zur Sammlung von Proben und genetischen Daten, zur Aufklärung und Einwilligung, über die Rechte der betroffenen Person und über die Treuhänder geforderten Maßnahmen bei der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen. Die Anzeige ist jeweils nach 5 Jahren mit einer Begründung der weiteren Speicherung zu erneuern. Ebenso sind die Vernichtung oder Löschung von Sammlungen nach Ziffer (1), die Löschung der Zuordnungsmerkmale bei Treuhändern und Trägerwechsel nach Ziffer (4) anzuzeigen.

Aufklärung und Einwilligung

(1) Die betroffene Person ist vor ihrer Einwilligung im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert (siehe oben), oder bei Sammlungen von Proben oder genetischen Daten (siehe oben) insbesondere aufzuklären über

- den verantwortlichen Träger des Forschungsvorhabens oder der Sammlung,
- das Ziel der Forschung oder bei Sammlungen die möglichen Forschungsrichtungen,
- ihre Rechte bei Patentanmeldungen und gewerblichen Nutzungen,

- die Dauer der Aufbewahrung von Proben und der Speicherung der genetischen Daten,

- Zeitpunkt und Art der Pseudonymisierung von Proben und genetischen Daten, sowie über die mögliche Wiederherstellung der Zuordnung zur betroffenen Person,

- ihr Recht - vorbehaltlich der pseudonymisierten Verarbeitung nach Beendigung des Forschungsvorhabens (siehe oben) - die Vernichtung der Probe und die Löschung der genetischen Daten oder die Aufhebung der Zuordnungsmöglichkeit zu verlangen, wenn sie die Einwilligung widerruft,

- ihr Recht, Ergebnisse von Untersuchungen nicht zur Kenntnis zu nehmen oder unter Nutzung eines darzustellenden Ent-Pseudonymisierungsverfahrens zu erfahren,

- ihr Recht, Auskunft über die zu ihr gespeicherten genetischen Daten zu verlangen.

Die Aufklärung hat schriftlich und mündlich zu erfolgen.

(2) Die Einwilligung soll die Entscheidung darüber umfassen, ob die betroffene Person vom Ergebnis der Untersuchung Kenntnis nehmen will oder nicht.

(3) Die Einwilligung kann eine Schweigepflichtentbindung für zu benennende behandelnde Ärzte einschließen, wenn die betroffene Person über Art und Umfang der Patientendaten informiert wird, die der Arzt für das Forschungsvorhaben (siehe oben) oder die Sammlung von Proben oder genetischen Daten (siehe oben) übermittelt.

Rechte der betroffenen Person

(1) Hinsichtlich der genetischen Daten stehen der betroffenen Person die im Bundesdatenschutzgesetz geregelten Rechte zu. Widerruft die betroffene Person ihre Einwilligung (siehe oben), sind entweder die Probe zu vernichten und die genetischen Daten zu löschen oder die Zuordnungsmerkmale zu löschen.

(2) Erbringt ein Forschungsvorhaben Ergebnisse, die für die betroffene Person von Bedeutung sind, veranlasst der Träger des Forschungsvorhaben eine Unterrichtung der betroffenen Person. Dies gilt nicht, wenn die betroffene Person erklärt hat, von dem Untersuchungsergebnis keine Kenntnis nehmen zu wollen (siehe oben).

Treuhänder

(1) Die Pseudonymisierung von Proben und genetischen Daten erfolgt durch einen Treuhänder. Er vergibt die Pseudonyme unverzüglich, verwahrt und verwaltet die Zuordnungsmerkmale und sichert die Rechte der betroffenen Person (siehe oben). Soweit erforderlich, kann er für diese Zwecke Kontakt mit der betroffenen Person aufnehmen. Er hat keinen Zugriff auf genetische Daten.

(2) Treuhänder kann eine natürliche Person sein, die von Berufs wegen einer besonderen Schweigepflicht unterliegt und vom Träger des Forschungsprojekts oder der Sammlung von Proben oder genetischen Daten unabhängig ist. Im Vertrag zwischen dem Treuhänder und dem Träger des Forschungsvorhabens oder der Sammlung von Proben oder genetischen Daten sind insbesondere die Anlässe und das Verfahren zur Wiederherstellung des Personenbezuges, die Nutzungsformen durch die Selbstkontrollgremien der Wissenschaft sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit festzulegen. Der Vertrag ist vorab der für die Datenschutzkontrolle zuständigen Behörde vorzulegen.

Schlussvorschläge

Ordnungswidrigkeit

Ordnungswidrig handelt, wer

- eine Reihenuntersuchung ohne die erforderliche Zulassung durchführt oder

- den Anzeigepflichten bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung von Proben oder genetischen Daten oder bei bestehenden Proben – oder genetischen Datensammlungen nicht fristgemäß nachkommt.

Straftaten

(1) Wer genetische Testverfahren unter Verstoß gegen die Anforderungen an das Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen einführt oder in Verkehr bringt

oder genetische Untersuchungen ohne eine individuelle Beratung öffentlich anbietet, wird mit ... ... bestraft. Handelt die Täterin oder der Täter gewerbsmäßig, ist die Strafe ... .

(2) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu medizinischen Zwecken durchführt, ohne

- Arzt oder Ärztin zu sein,

- die für die genetischen Untersuchungen zu medizinischen Zwecken festgelegten Beschränkungen der Untersuchungszwecke einzuhalten,

- die geforderte Aufklärung und Beratung unternommen bzw. sichergestellt zu haben oder

- die Einwilligung der betroffenen Person eingeholt zu haben,

wird mit ... ... bestraft.

(3) Wer als Arbeitgeber oder als Versicherer gegen das Verbot genetischer Untersuchungen verstößt, ohne dass die vorgesehene Ausnahmeregelung eingreift, wird mit ... ... bestraft.

(4) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu Zwecken der Abstammungsklärung oder Identifizierung in unzulässiger Weise auf prädiktive oder diagnostische Ziele ausrichtet oder ohne die geforderte Einwilligung durchführt, wird mit ... ... bestraft.

(5) Wer vorsätzlich oder fahrlässig personenbeziehbare Proben, DNS-/RNS-Teile oder genetische Daten entgegen den Regelungen für genetische Untersuchungen zu Forschungszwecken

- ohne Einwilligung oder Aufklärung zu Forschungszwecken nutzt oder

- in Sammlungen für Forschungszwecke zur Verfügung stellt,

wird mit ... ... bestraft.

Antrag

Die oben aufgeführten Straftaten werden nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person und die für die Datenschutzkontrolle zuständige Behörde.

Befristung

Die Regelungen sind auf zehn Jahre zu befristen. Acht Jahre nach In-Kraft-Treten haben die für die Datenschutzkontrolle zuständigen Behörden unter Federführung des Bundesbeauftragten für den Datenschutz dem Gesetzgeber einen Bericht über die Wirksamkeit der vorgeschlagenen Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht sowie zu möglichen Rechtsvereinfachungen vorzulegen. Diesem Bericht sind Stellungnahmen des Ethikrates und der Deutschen Forschungsgemeinschaft beizufügen.

Übergangsvorschrift

Träger von bestehenden Proben- und genetischen Datensammlungen haben der Anzeigepflicht bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung innerhalb von sechs Monaten nach In-Kraft-Treten dieses Gesetzes nachzukommen. Innerhalb dieser Frist ist den Anforderungen an die Einwilligung zu entsprechen. Vor In-Kraft-Treten dieses Gesetzes ohne Einwilligung gewonnene Proben und erhobene genetische Daten sind spätestens nach zwei Jahren zu vernichten bzw. zu löschen. Dies ist der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen.

Anlage 13: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001 zur LKW-Maut auf Autobahnen und zur allgemeinen Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen.

Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

- Es ist sicherzustellen, dass anfallende personenbezogenen Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen

Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

Anlage 14: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001 zur „neuen Medienordnung“

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

Anlage 15: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001: Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus – mit den Worten des Bundesverfassungsgerichts – auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene

sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anlage 16: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001: Biometrische Merkmale in Personalausweisen und Pässen

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u.a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Not-

wendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

Anlage 17: Grundsatzpapier der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001: Grundsätze zur Übermittlung von Telekommunikationsverbindungsdaten

Die Bundesregierung hat den Gesetzentwurf für eine Nachfolgeregelung zu § 12 FAG vorgelegt, der eine Reihe datenschutzrechtlich positiver Ansätze enthält. Der Bundesrat hat sich demgegenüber in seiner Stellungnahme für eine Regelung ausgesprochen, die wesentlichen datenschutzrechtlichen Anforderungen nicht gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder lehnen den Vorschlag des Bundesrates entschieden ab.

Sie halten es für nicht vertretbar, Auskünfte über zurückliegende Aktivmeldungen von Mobiltelefonen auch bei reinem Stand-by-Betrieb zu erteilen und Diensteanbieter zur Aufzeichnung von Telekommunikationsverbindungsdaten eigens für Zwecke der Strafverfolgung zu verpflichten.

Auch die vom Bundesrat vorgeschlagene Regelung des § 18a BVerfSchG zur Übermittlung von Telekommunikationsverbindungsdaten an die Verfassungsschutzbehörden halten die Datenschutzbeauftragten des Bundes und der Länder für nicht akzeptabel. Sie fordern eine deutliche Klarstellung im Wortlaut des Gesetzes, dass Verbindungsdaten an den Verfassungsschutz nur dann übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine in § 3 Abs. 1 G 10 genannte Straftat plant, begeht oder begangen hat oder sonst an gewalttätigen Bestrebungen oder sicherheitsgefährdenden Tätigkeiten teilnimmt. Eine Übermittlung der Verbindungsdaten für den gesamten Aufgabenbereich des Verfassungsschutzes ginge dagegen erheblich zu weit.

Ferner halten es die Datenschutzbeauftragten für geboten, hinsichtlich der Kennzeichnung und Zweckbindung der Daten, der Mitteilungen an Betroffene und der parlamentarischen Kontrolle einen dem G 10 möglichst gleichwertigen Standard zu gewährleisten.

Die Bundesregierung und der Deutsche Bundestag werden gebeten, diese datenschutzrechtlichen Mindestanforderungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

Anlage 18: Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. – 26.10.2001: EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von

EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

- Informationsaustausch mit Partnern
  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und –stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

- Verarbeitung personenbezogener Daten
  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

- Ermittlungsindex und Dateien
  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

- Auskunftsrecht
  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer

Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

- Änderung, Berichtigung und Löschung
  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

- Speicherungsfristen
  Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z.B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

- Datensicherheit
  Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

- Gemeinsame Kontrollinstanz
  Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindenden Charakter haben.

- Rechtsschutz
  Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

- Rechtsetzungsbedarf
  Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermitt-

lungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.
Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anlage 19: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.03.2002: Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z.B. Krankheits, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den

Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

Anlage 20: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.03.2002: Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet.

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

Anlage 21: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.03.2002: Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz „Für eine freie Telekommunikation in einer freien Gesellschaft“) darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 01.01.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z.B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte und Verbindungs- aufzuzeichnen und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für

eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anlage 22: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.03.2002: Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 23: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24.05.2002: Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der ge-

schäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die

Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z.B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und

vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anlage 24: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002: Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Anlage 25: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002 zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebensowenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 26: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002 zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Abkürzungsverzeichnis

Abl.	Amtsblatt (der Europäischen Union)
Abs.	Absatz
ADO	Allgemeine Dienstordnung
ADV	Automatisierte Datenverarbeitung
AFGIB	Arbeitsgemeinschaft zur Förderung der Geriatrie in Bayern
AGKRG	Gesetz zur Ausführung des Krebsregistergesetzes
AGO	Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
ALB	Automatisiertes Liegenschaftsbuch
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
BÄK	Bundesärztekammer
BAQ	Bayerische Arbeitsgemeinschaft für Qualitätssicherung in der stationären Versorgung
BauGB	Baugesetzbuch
BayArchivG	Bayerisches Archivgesetz
BayBesG	Bayerisches Besoldungsgesetz
BayBG	Bayerisches Beamtengesetz
BayBO	Bayerische Bauordnung
BayDAV	Dienstanschlussvorschriften
BayDSG	Bayerisches Datenschutzgesetz
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayGlG	Bayerisches Gleichstellungsgesetz
BayHO	Bayerische Haushaltsordnung
BayKOM	Bayerisches Kommunikationsnetz
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
BestG	Bestattungsgesetz
BFD	Bezirksfinanzdirektion
BfD	Der Bundesbeauftragte für den Datenschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGK	Bayerische Gesundheitschipkarte und Kommunikation
BGSG	Bundesgrenzschutzgesetz
BISS	Benutzerbestimmbare Informationsflusskontrolle
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
bspw.	beispielsweise
BT-Drs.	Bundestagsdrucksache
BtmG	Betäubungsmittelgesetz
BÜVO	Beitragsüberwachungsverordnung
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BYBN	Bayerisches Behördennetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
CA	Certification Authority
CC	Common Criteria
CD-ROM	Compaktdisk – Read Only Memory
CERT	Computer Emergency Response Team
CHAP	Callenge Authentication Protocol
CISO	Chief Information Security Officer
DAE	Deutsche Arbeitsgemeinschaft für Epidemiologie
DECT	Digital European Cordless Telephone
DFG	Deutsche Forschungsgemeinschaft
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DGSMP	Deutsche Gesellschaft für Sozialmedizin und Prävention
dkfz	Deutsches Krebsforschungszentrum
DMP	Disease-Management-Programme (Strukturierte Behandlungsprogramme)

DNA-Analyse	Molekulargenetische Untersuchung
DSRV	Datenstelle der Rentenversicherungsträger
DV	Datenverarbeitung
DVBl	Deutsches Verwaltungsblatt
DVKRG	Verordnung zur Durchführung des Krebsregistergesetzes
EA	Errichtungsanordnung für Dateien
EDV	Elektronische Datenverarbeitung
EDVG	EDV-Gesetz des Freistaates Bayern
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
EGG	Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr – Gesetz)
EGMR	Europäischer Gerichtshof für Menschenrechte
ELSTER	Elektronische Steuererklärung
EStG	Einkommensteuergesetz
EU	Europäische Union
FAG	Fernmeldeanlagengesetz
FAQ	Frequently Asked Questions (Häufig gestellte Fragen)
ff.	folgende
FTAM	File Transfer, Access and Management
FTP	File Transfer Protocol
G-10-Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz)
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GAST-Dateien	Dateien zur Gefahrenabwehr und Strafverfolgung
gem.	Gemäß
GEWAN	Gewerbeanzeigen im Netz
GG	Grundgesetz
ggf.	gegebenenfalls
GiB-DAT-Projekt	Geriatrie-in-Bayern-Datenbank
GKV	Gesetzliche Krankenversicherung
GLKrWG	Gemeinde- und Landkreiswahlgesetz
GMDS	Deutsche Gesellschaft für medizinische Information, Biometrie und Epidemiologie
GO	Gemeindeordnung
GRUBIS	Grundstücks- und Bodeninformationssystem
GSM	Global System for Mobile Communications
GTH	Gesellschaft für Thrombose- und Hämestaseforschung e.V.
GVBl	Gesetz- und Verordnungsblatt
GVG	Gesellschaft für Versicherungswissenschaft und -gestaltung e.V.
HCP-Protokoll	Health Care Professional Protokoll

HGP	Humangenomprojekt
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IBP	Informationssystem der Bayerischen Polizei
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronical Engineers
IfSG	Infektionsschutzgesetz
IfSG	Infektionsschutzgesetz
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	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste
IuKG	Gesetz über den Einsatz der Informations- und Kommunikationstechnik in der öffentlichen Verwaltung (Bayern)
IuK-Systeme	Informations- und Kommunikationssysteme
JuMiG	Justizmitteilungsgesetz
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KBV	Kassenärztliche Bundesvereinigung
KBV	Kassenärztliche Bundesvereinigung
KHG	Krankenhausfinanzierungsgesetz
KIS	Krankenhausinformations- und Kommunikationssystem
KMBek	Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus
KMS	Schreiben des Bayerischen Staatsministeriums für Unterricht und Kultus
KORA	Kooperative Gesundheitsforschung in der Region Augsburg
KRG	Krebsregistergesetz des Bundes (bis 31.12.1999)
KTQ	Kooperation für Transparenz und Qualität im Krankenhaus
KV	Kassenärztliche Vereinigung
KVB	Kassenärztliche Vereinigung Bayerns
KVK	Krankenversichertenkarte
KVR	Kreisverwaltungsreferat
KWMBl I	Kultus- und Wissenschaftsministerialblatt Teil I
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
MSD	Medizinisch-Sozialpädagogische Dienste (Fachdienste bei den Bezirken)
MUCK	Multifunktionale Chipkarte
MWG `92	Münchner Weltwirtschaftsgipfel 1992
NAT	Native Address Translation
Nds.	Niedersächsisch
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
o.e.	oben erwähnt
o.g.	oben genannt
ODSP	Online-Datenschutz-Prinzipien
OSS	Online Service System; SAP-Fernwartung
P3P	Platform for Privacy Preferences
PAG	Bayerisches Polizeiaufgabengesetz
PC	Personalcomputer
PD	Polizeidirektion
PFAD	Personen- und Fall-Auskunftsdatei
PGP	Pretty Good Privacy
PHW	Personenbezogener Hinweis
PIN	Personal identification number
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
RSAV	Risikostruktur-Ausgleichsverordnung
RV	RV Rentenversicherung
S.	Seite
S/MIME	Secure Multipurpose Internet Mail Extensions
SAP	Systems, Applications, and Products
SDBY	Staatsschutzdatei Bayern
SDÜ	Schengener Durchführungsabkommen
SGB	Sozialgesetzbuch

SigG	Signaturgesetz
SigV	Signaturverordnung
SIS	Schengener Informationssystem
SozhiDAV	Sozialhilfedatenabgleichsverordnung
SSID	Server Set ID
SSL	Secure Sockets Layer
STARIS	Staatsanwaltschaftliches Registrierungs- und Informationssystem
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
StMAS	Bayerisches Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen
StPO	Strafprozessordnung
StVÄG	Strafverfahrensänderungsgesetz
StVG	Strassenverkehrsgesetz
TB	Tätigkeitsbericht
TCP/IP	Transmission Control Protocol/Internet Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TKLGebV	Telekommunikationslizenzgebührenverordnung
TMSI	Temporary Mobile Subscriber Identity
TOA	Täter-Opfer-Ausgleich
TTP	Trusted Third Parties
TÜ	Telefonüberwachung
u.a.	unter anderem
URL	Uniform Resource Locator (Universal Resource Locator)
UStG	Umsatzsteuergesetz
UVT	Unfallversicherungsträger
VAwS	Verordnung zum Umgang mit wassergefährdenden Stoffen
VBG 100	Unfallverhütungsvorschrift Arbeitsmedizinische Vorsorge
vbs	Visual Basic Script
VDR	Verband Deutscher Rentenversicherungsträger
VersammlG	Versammlungsgesetz
VersammlG	Versammlungsgesetz
VGemO	Verwaltungsgemeinschaftsordnung
VGH	Verwaltungsgerichtshof
vgl.	Vergleiche
ViCLAS	Violent Crime Linkage Analysis System (Analyse-System zur Verknüpfung von Gewaltverbrechen)
VPN	Virtual Private Network
VSA	VSA Verrechnungsstelle der Süddeutschen Apotheken GmbH
VwVfG	Verwaltungsverfahrensgesetz
W3C	World Wide Web Consortium
WaffG	Waffengesetz
WEP	Wired Equivalent Privacy

WLAN	Wireless Local Area Network
WWW	World Wide Web
XML	Extended Markup Language
z.B.	zum Beispiel
ZPO	Zivilprozessordnung
ZStV	Zentrales staatsanwaltschaftiches Verfahrensregister

Stichwortverzeichnis