Bayerischer Landtag
15. Wahlperiode
Drucksache 15/**2074**
27.01.2005

21. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

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

Berichtszeitraum 2003/2004

Der Bayerische Landesbeauftragte für den Datenschutz

Nr. DSB/1 – 510 – 22 München, 27.01.2005

An den
Präsidenten
des Bayerischen Landtags
Herrn Alois Glück

81627 München

21. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident,

in der Anlage übersende ich gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes den 21. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit freundlichen Grüßen

Reinhard Vetter

1 Schwerpunkte im Berichtszeitraum

Die Jahre 2003 und 2004 waren, wie auch die vorhergehenden Jahre, von einer Fülle von Einzelfragen und -problemen, aber auch von großen Gesamtkomplexen geprägt. Zu einigen Schwerpunkten verweise ich auf Nachstehendes, zu ausgewählten wichtigen Einzelfragen auf nachstehende Übersicht (Nr. 2) und insgesamt auf den Tätigkeitsbericht im Einzelnen.

1.1 Der Sicherheitsbereich

Als ein großer Gesamtkomplex hat sich auch im Berichtszeitraum wieder der Sicherheitsbereich erwiesen. Dieser war von zwei Momenten geprägt: Einmal die nach wie vor bestehende Bedrohung durch den internationalen islamistischen Terrorismus, zum anderen aber auch durch die Bestrebungen des Bayerischen Innenministeriums, zur Verbesserung der Tätigkeit der Polizei vor allem im präventiven Bereich vermehrt Mittel der modernen Technik einzusetzen.

1.1.1 Die Bedrohung durch den internationalen Terrorismus

Die Bedrohung durch den internationalen Terrorismus hat die Frage einer verbesserten Zusammenarbeit zwischen den Verfassungsschutzbehörden und der Polizei aufgeworfen und zwar auf Bundes- wie auf Landesebene. Ich habe mich relativ früh mit dieser Problematik befasst, da ich der Meinung bin, dass auch von Seiten des Datenschutzes die Frage gestellt und beantwortet werden muss, ob die verfassungsrechtlichen Möglichkeiten, insbesondere die von Grundgesetz und Bayerischer Verfassung gesetzten Grenzen, eine Verbesserung der Zusammenarbeit von Polizei und Verfassungsschutz erlauben. Ich bin zu dem Ergebnis gekommen, dass das der Fall ist, und habe diese Auffassung in die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingebracht.

1.1.2 Der vermehrte Einsatz technischer Mittel

Das Bayerische Innenministerium hat zum einen die Video-Beobachtung öffentlicher Räume weiter vorangetrieben. Ich habe in meiner Stellungnahme zur Vollzugsbekanntmachung (Nr. 7.13) verschiedene Einwände erhoben, u.a. zur Begrenzung der Zugriffsrechte und Protokollierung und zu der Umschreibung der Örtlichkeiten für Videoüberwachung, die vom Innenministerium leider nicht aufgenommen wurden. Gegen die konkret installierten Videoanlagen erhob ich keinen Widerspruch, da die gesetzlichen Voraussetzungen - jeweils besonders kriminalitätsbelastete Orte - nachgewiesen werden konnten. Diskussionspunkte waren aber u.a. die ausreichenden Hinweise auf die Beobachtung und die Dokumentation der Auswertungen von Aufzeichnungen.

Weiter befassen musste ich mich auch mit der Idee des Bayerischen Innenministeriums, die Kennzeichen vorbeifahrender Kraftfahrzeuge in bestimmten Bereichen fotografisch zu erfassen und nach Digitalisierung mit polizeilichen Dateien abzugleichen. Das Bayerische Innenministerium ist inzwischen meiner Forderung nach einer gesetzlichen Grundlage für diese Maßnahmen gefolgt. Gegen die Absicht, solche Abgleiche auf gesetzlicher Grundlage grundsätzlich nur mit Fahndungsdateien durchzuführen und „Nichttrefferfälle“ sofort zu löschen, habe ich mich nicht ausgesprochen. Im Laufe mehrerer Besprechungen habe ich verlangt, dass die Beschränkung auf Fahndungsdateien und allenfalls auf Dateien, deren Abfrage zur Bewältigung von Gefahren in Bezug auf bestimmte Ereignisse erforderlich ist, und die sofortige Löschung von „Nichttrefferfällen“ in der Novelle zum Polizeiaufgabengesetz (PAG) klar und unmissverständlich zum Ausdruck kommt. Das Innenministerium ist diesen Forderungen nachgekommen.

Ebenfalls in der Novelle zum PAG vorgesehen ist der präventive Einsatz der Telekommunikationsüberwachung durch die Polizei. Ich habe mich gegen dieses Vorhaben nicht grundsätzlich ausgesprochen, da ich zur Kenntnis nehmen muss, dass die Polizei das tiefer eingreifende Mittel der Wohnraumüberwachung zur Verhinderung von Straftaten im Polizeiaufgabengesetz bereits hat. Wenn die polizeiliche Aufgabe Straftaten zu verhindern dieses ultimative Mittel gesetzlich rechtfertigt, dann sehe ich auch die Möglichkeit, gesetzlich das mildere Mittel der Telekommunikationsüberwachung einzuführen. Im Übrigen hat auch das Bundesverfassungsgericht die präventive TKÜ grundsätzlich für zulässig angesehen. Wesentlich sind klare gesetzliche Schranken, damit die präventive TKÜ nicht ausufert. Weiter sind auch für die präventive Wohnraumüberwachung wie auch für die neu einzuführende präventive Telekommunikationsüberwachung die Grundsätze des Bundesverfassungsgerichts in seinem Urteil zur akustischen Wohnraumüberwachung zur Strafverfolgung zu beachten. Ich habe deshalb für die Novelle des PAG u.a. das Einhalten eines engen geschlossenen Straftatenkatalogs und auf Tatsachen beruhende objektive Anhaltspunkte für eine bevorstehende Begehung solcher Straftaten gefordert. Weiter ist der Schutz von Berufsgeheimnisträgern und von besonderen Vertrauensverhältnissen zu gewährleisten. Das Innenministerium hat in mehreren Gesprächen wesentliche Forde-

rungen von mir aufgenommen. Einzelne Punkte sind offen geblieben.

Insgesamt erfordert die Entwicklung im Sicherheitsbereich große Aufmerksamkeit des Datenschutzbeauftragten. Gestiegene Gefährdungen haben regelmäßig intensivere Maßnahmen der Sicherheitskräfte zur Folge. Die sich ständig verbessernden technischen Möglichkeiten der Datenerhebung und weiteren Verarbeitung ermöglichen auch von der technisch organisatorischen Seite immer weitere und tiefere Eingriffe. Davon sind in immer vermehrtem Maße in großem Umfang auch Bürgerinnen und Bürger betroffen, die für diese Maßnahmen keinen Anlass gegeben haben. Das kann sich durchaus zum Nachteil der Betroffenen auswirken, wie auch Einzelbeispiele meiner Kontrolltätigkeit zeigen. Der Satz „ich habe nichts zu verbergen, also betrifft mich das nicht“ stimmt deshalb nicht. Ein solches Betroffensein lässt sich nicht immer vermeiden, bei Maßnahmen wie dem Kennzeichenscanning oder der Videobeobachtung ist es sogar die Regel. Eingreifende Maßnahmen müssen gesetzlich auf das unbedingt erforderliche Maß unter Wahrung der Verhältnismäßigkeit begrenzt werden. Das gilt im Besonderen für solche, die auch Bürgerinnen und Bürger betreffen, die für solche Maßnahmen keinen Anlass gesetzt haben. Die Aufgabe des Datenschutzbeauftragten ist deshalb nicht leichter geworden.

Ich begrüße es deshalb sehr, dass die von mir im letzten Tätigkeitsbericht kritisch angesprochenen weiteren Verschärfungen des Terrorismusbekämpfungsgesetzes nicht realisiert wurden.

1.2 Die Gesundheitskarte

Als Vorsitzender des Arbeitskreises „Gesundheit, Soziales“ hatte ich mich wiederum mit dem Komplex „Gesundheitskarte“ zu befassen. Die Einführung der „Gesundheitskarte“ als Träger nicht nur von Verwaltungsdaten, sondern auch als Medium zur Übermittlung von Rezepten und in weiteren Ausbaustufen als Träger von medizinischen Informationen bzw. als Zugangsmittel zu Speicherungen solcher Informationen auf Servern stellt ein höchst komplexes Vorhaben dar, dessen Einführung zum 01.01.2006 auch für die Grundkonfiguration, bestehend aus den Pflichtanwendungen Verwaltungsdaten und elektronisches Rezept, ein sehr ehrgeiziges Ziel ist. An der Realisierung dieses Konzepts arbeiten diverse Gremien, was die Teilnahme der Datenschutzseite nicht leichter macht. Zur datenschutzrechtlichen Begleitung des Vorhabens wurde eine Unterarbeitsgruppe des AK Gesundheit und Soziales und des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gegründet, dessen Mitglied ich bin. Wesentliches Ziel der Arbeitsgruppe ist es, die rechtlich in § 291 a SGB V vorgesehenen Entscheidungsrechte des Patienten, wer in welchem Umfang Zugriff auf seine medizinischen Daten haben soll, auch in der technischen Umsetzung einzufordern. Ich halte die effektive Umsetzung dieser gesetzlichen Forderungen der Sicherung des Selbstentscheidungsrechts der Patienten, die auf Forderungen der Datenschutzkonferenz des Bundes und der Länder beruhen, für eine ganz wesentliche Voraussetzung dafür, dass die Hoheit des Patienten über seine medizinischen Daten erhalten bleibt. Kern dieser Patientenhoheit ist es, dass er selbst entscheiden kann, welchem Arzt/Apotheker er seine medizinischen Daten, d.h. intime Angaben über seine Person, anvertraut. Diese Patientenhoheit muss auch unter der Anwendung neuzeitlicher Mittel der Informationsverarbeitung, wie der Gesundheitskarte mit ihren freiwilligen Anwendungen „elektronischer Arztbrief“ und „elektronische Patientenakte“ erhalten bleiben. Die Informationstechnik soll den Patienten in der Wahrnehmung seiner Rechte unterstützen, nicht ihn entmündigen. Sie darf deshalb die informationellen Rechte des Patienten und der Patientin nicht verschlechtern. Diese von mir formulierte Grundforderung war Grundlage des Beschlusses der 50. Datenschutzkonferenz, auf der die wesentlichen Forderungen an die Gesundheitskarte formuliert wurden und die in § 291 a SGB V Eingang gefunden haben. Zum Redaktionsschluss dieses Beitrags war die Umsetzung der technischen Konzeption der Gesundheitskarte, insbesondere auch die Entscheidung der Frage, ob eine rein kartenbasierte, eine rein serverbasierende oder eine Mischlösung realisiert werden soll, noch nicht abgeschlossen. Aus technischen Gründen (u.a. Speicherkapazität der Karte) wird wohl eine Mischlösung in Frage kommen. Dagegen bestehen keine Bedenken, wenn durch geeignete Sicherheitsmechanismen wie Verschlüsselungstechnologien und Zugriffsschutz auch in der Hand des Patienten sichergestellt werden kann, dass Zugriff auf die Gesundheitsdaten nur mit Zustimmung des Patienten genommen werden kann (Nr. 6.1). Die mit der Entwicklung und dem Einsatz der Gesundheitskarte verbundenen Fragen zeigen einmal mehr die Notwendigkeit des Zusammenführens der datenschutzrechtlichen Zuständigkeiten für den öffentlichen und privaten Bereich in einer Hand. Ein Hauptanwendungsfeld der Gesundheitskarte ist mit den niedergelassenen Ärzten und den Apotheken der private Bereich, für den ich gar nicht zuständig bin.

1.3 Das JobCard-Verfahren

Das Bundeswirtschaftsministerium plant die Einführung einer zentralen Speicherstelle, in der Arbeits- und Einkommensdaten der gesamten abhängig erwerbstätigen Bevölkerung Deutschlands gespeichert werden sollen. Sinn dieser zentralen Datenbank soll

die Entlastung der Wirtschaft sein, die zurzeit entsprechende Bescheinigungen ausstellen muss, wenn staatliche bzw. kommunale Leistungen wie Arbeitslosengeld, Wohngeld, Kindergeld, usw. beantragt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ihre Arbeitskreise AK Gesundheit und Soziales und AK Technik beauftragt, dieses Vorhaben datenschutzrechtlich zu begleiten. Die Arbeitskreise haben auf meine Anregung hin eine gemeinsame Arbeitsgruppe gebildet, deren Moderation mir übertragen wurde. Die in der Arbeitsgruppe vertretenen Landesbeauftragten für den Datenschutz haben gegenüber der vom Bundeswirtschaftsministerium mit der Ausarbeitung eines Konzeptes beauftragten Informationstechnischen Servicestelle der gesetzlichen Krankenkassen -ITSG- eine Revision des bisherigen Konzeptes gefordert mit dem Ziel, die schon bisher vorgesehene Verschlüsselung der Daten in die Hände der betroffenen Beschäftigten zu geben. Mit dieser Maßnahme soll das Risiko einer Zweckentfremdung oder eines Missbrauchs einer derartigen zentralen Datenbank mit sensiblen Daten minimiert werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 68. Sitzung in Saarbrücken inzwischen beschlossen, dass das Bundeswirtschaftsministerium gebeten werden soll, die Realisierbarkeit dieses Konzepts durch einen neutralen Gutachter zu überprüfen. Sollte dieses Konzept nicht zu realisieren sein, wird an einer datenschutzrechtlichen Verbesserung im Rahmen des bisherigen Konzeptes gearbeitet (Nr. 22.2.3.3).

1.4 Die Telematikplattform für medizinische Forschungsnetze (TMF e.V.)

Die TMF e.V. ist ein Zusammenschluss von Forschungsverbünden und überregional arbeitenden Einrichtungen zur medizinischen Forschung. Ziel der TMF ist die Koordination und Vertretung der Interessen der vernetzten Forschung, sowie die Schaffung forschungsfördernder Strukturen. Seit 1999 wurde die TMF als Interessensgemeinschaft durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert. Mit Schreiben des Bundesministeriums für Bildung und Forschung vom 29.01.2002 wurde ich zum Mitglied des seinerzeitigen Koordinierungsrates berufen. Im Zuge der Umgründung in einen rechtsfähigen Verein wurde ich von der Mitgliederversammlung zum Mitglied des Beirats gewählt, damit die Anforderungen des Datenschutzes in die Verarbeitung medizinischer Daten zu Zwecken der Forschung in die Entscheidungsprozesse eingebracht werden. Auf meine Anregung und unter Mitwirkung meiner Mitarbeiter wurde von der TMF ein Datenschutzkonzept entwickelt, das - ggf. unter Anpassung - der Datenverarbeitung der verschiedenen Forschungsverbünde zu Grunde gelegt werden kann. Ziel dieses Datenschutzkonzeptes ist es, eine sinnvolle Nutzung medizinischer Daten in vernetzten Datenbeständen unter Beachtung der ärztlichen Schweigepflicht und des Rechts auf informationelle Selbstbestimmung des Patienten zu ermöglichen. Dies wird durch eine Kombination von Einwilligung, Trennung von Identifikations- und medizinischen Daten und Pseudonymisierungsverfahren erreicht. Mit der Zugrundelegung dieses von dem Arbeitskreis Wissenschaft der Datenschutzkonferenz konsentierten Datenschutzkonzeptes wird die datenschutzrechtliche Begleitung der Forschungsverbünde, deren Umfang immer mehr zunimmt, wesentlich vereinfacht.

2 Überblick

2.1 Übersicht über weitere wesentliche Punkte des Berichtszeitraums

2.1.1 Polizeibereich

- Meine Bemühungen zur datenschutzgerechten Gestaltung des KAN habe ich fortgesetzt. Trotz gewisser Verbesserungen (siehe auch Nr. 2.1.1 20. Tätigkeitsbericht) bestehen immer noch Mängel (Nr. 7.1). So reichen die Regelbeispiele für Fälle „geringerer Bedeutung“ nicht aus; dies kann sich wegen der längeren Speicherfristen für die Betroffenen sehr nachteilig auswirken. Sehr restriktive Formulierungen in den Vorgaben lassen befürchten, dass Speicherungen im KAN auch dann nicht gelöscht werden, wenn der strafprozessuale Anfangsverdacht vernünftigerweise nicht mehr aufrecht erhalten werden kann; das bedeutet eine Schlechterstellung des Betroffenen als nach dem PAG geboten ist. Es erfolgt auch keine Speicherung des Verfahrensausganges im KAN, was für den Fall eines Datenabgleichs durch einen Polizeibeamten wesentliche Nachteile für den Betroffenen hat: Der Beamte erfährt dann im Rahmen des Datenabgleichs nichts über einen Freispruch oder eine Verfahrenseinstellung, was eine erheblich negativere Einschätzung durch ihn zur Folge hat. Schließlich ist in den einschlägigen Richtlinien nach wie vor nicht ausdrücklich festgelegt, dass das „Ob“ der Speicherung nach Abschluss der Ermittlungen nochmals zu prüfen ist. Das kann zur Folge haben, wie das in einem Fall geschehen ist, dass der Betroffene auf Grund einer Speicherung vor Augen seines Arbeitgebers einer für ihn entwürdigenden Durchsuchung unterzogen wird, obwohl er nach dem Ergebnis der Ermittlungen als Täter nicht in Betracht kam (S. 30). Fast skurril ist der Fall, in dem wegen einer Änderung der Deliktsbezeichnung (ursprünglich „Gefähr-

dung des Straßenverkehrs“, im weiteren „Gefährdung des Straßenverkehrs infolge Alkohol“) im Zug einer Umstellung des Straftatenkatalogs dem Betroffenen bei einer Sicherheitsüberprüfung im Ausland letzteres vorgehalten wurde, was natürlich zu einer völlig anderen Einschätzung der dortigen Behörden geführt hat. In diesem Fall hat das Landeskriminalamt auf meine Aufforderung diesen und Parallelfälle berichtigt.

- Ein Dauerthema ist auch die „Polizeiliche Sachbearbeitung/Vorgangsverwaltung – Verbrechensbekämpfung“. Über die Doppelfunktion dieser Datei – einerseits Dokumentation der Vorgänge, andererseits auch Grundlage der polizeilichen Sachbearbeitung – hatte ich mehrfach in früheren Jahren berichtet. Von den zahlreichen Problemen möchte ich wegen ihrer allgemeinen Bedeutung hier auf zwei hinweisen: Die Zugriffsberechtigung wurde erneut ausgeweitet auf landesweiten Zugriff für bestimmte Sachgebiete des Landeskriminalamts und für bestimmte Funktionen der Polizei, ohne dass die Erforderlichkeit für einen landesweiten Zugriff auf personenbezogene Daten von nur regionaler Bedeutung ausreichend dargetan wäre. Das Innenministerium hat auf meinen Vorhalt immerhin eingeräumt, dass es die Verbände bei der Umsetzung auf die „erforderliche Sensibilität“ bei der Vergabe von Zugriffsberechtigungen hinweisen werde. Für inhaltlich bedeutsam halte ich die Weigerung des Innenministeriums, den Ausgang eines Verfahrens in der Vorgangsverwaltung zu speichern: Eine Ingewahrsamnahme war für rechtswidrig erklärt worden, die Speicherung dieses Ergebnisses wurde mit der Begründung verweigert, dass dies an der Existenz des Vorgangs nichts ändere und der Ausgang aus der Akte ersehen werden könne. Ich halte diese Begründung für völlig verfehlt, da sie überhaupt nicht auf die Funktion der PSV auch als Grundlage der polizeilichen Sachbearbeitung eingeht (Nr. 7.2).

- Immer wieder muss ich mich mit unzulässigen Abfragen aus dem polizeilichen Informationssystem aus privaten Anlässen befassen (Nr. 7.19). So hat ein Polizeibeamter in seiner Eigenschaft als Vermieter Daten seiner Mieterin aus dem Einwohnermelderegister abgefragt, ein anderer Daten aus dem zentralen Verkehrsinformationssystem, um einem Bekannten einen Gefallen zu tun. Solche unzulässigen Nutzungen polizeilicher und anderer staatlicher oder kommunaler Dateien aus privaten Motiven muss unterbunden werden, auch da sie das Vertrauen in die Sauberkeit der öffentlichen Verwaltung erheblich belasten. Ich habe deshalb kein Verständnis dafür, dass es das Innenministerium bisher abgelehnt hat, neben der Protokollierung von Abfragen weitere von uns vorgeschlagene Schranken, wie z.B. die notwendige Angabe des Aktenzeichen eines zu Grunde liegenden Vorgangs oder/und eines Stichworts zum Grund der Abfrage (wie schon bei ZEVIS) einzuführen. Die Protokollierung ohne näheren Hinweis reicht vielfach nicht aus (nachträgliche Erklärung „aus dienstlichem Anlass“).

2.1.2 Verfassungsschutz

Bei meinen Prüfungen des Verfassungsschutzes habe ich festgestellt, dass die gesetzlichen Voraussetzungen für die Datenverarbeitung im Wesentlichen beachtet werden (Nr. 8.2).

Das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung erfordert auch eine Änderung der Regelung heimlicher Überwachungsmaßnahmen nach dem Bayerischen Verfassungsschutzgesetz. Das Staatsministerium des Innern hat sich dieser Beurteilung für die Wohnraumüberwachung angeschlossen. Das Ministerium hat dem Landtag über die Frage der Änderung des Bayerischen Verfassungsschutzgesetzes grundsätzlich berichtet und mitgeteilt, dass an einer Änderung des Bayerischen Verfassungsschutzgesetzes gearbeitet wird.

Für sonstige heimliche Überwachungsmaßnahmen lehnt es eine Anwendung des Urteils ab, da nach seiner Auffassung die Eingriffsintensität bei Observationen geringer sei, als bei der Wohnraumüberwachung. Dies muss m.E. im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts überprüft werden, da der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung nicht auf privaten Wohnraum beschränkt sein kann. Ich habe das Ministerium hierauf hingewiesen (Nr. 8.1).

2.1.3 Justiz

Aus diesem Bereich hebe ich hier den Entwurf der Bundesregierung für ein Justizkommunikationsgesetz und einen bemerkenswerten Einzelfall hervor. In meiner Stellungnahme zu dem Justizkommunikationsgesetz-Entwurf gegenüber dem Staatsministerium der Justiz habe ich besonders die unzureichenden Sicherheitsmaßnahmen (u.a. keine Pflicht zur Datenverschlüsselung) bemängelt (Nr. 9.1.1). Es erscheint

mir höchst misslich, dass im staatlichen Bereich in einem Feld der Verarbeitung sensibler privater Daten, z.B. über familienrechtliche oder vermögensrechtliche Auseinandersetzungen, die für die Verarbeitung sensibler digitaler Daten nach dem Stand der Technik angemessenen Sicherheitsmaßnahmen nicht vorgeschrieben werden. In dem bemerkenswerten Einzelfall musste ich ein Amtsgericht beanstanden, in dem für die Vorbereitung eines Personalgesprächs mit einer Angestellten die Akte über ihr Scheidungsverfahren, das ebenfalls bei diesem Gericht anhängig war, beigezogen wurde. Auch das gut gemeinte Motiv, private Belastungen in dem Gespräch zu berücksichtigen, rechtfertigte die Kenntnisnahme der privatesten Daten nicht, die oft in einer Scheidungsakte enthalten sind. Das Amtsgericht hat sich bei der betroffenen Frau entschuldigt.

2.1.4 Kommunales und Meldewesen

Ich nenne hier wegen ihrer allgemeinen Bedeutung drei Fragenbereiche. Die durch die Internettechnologie gegebenen Möglichkeiten der Öffentlichkeitsarbeit verstellen manchmal den Blick auf das datenschutzrechtlich Zulässige: So musste ich die Aufnahme der Namen und Geburtstage neugeborener Gemeindekinder in das Internetangebot einer Gemeinde ohne Zustimmung der Eltern beanstanden (Nr. 11.3). In einem anderen Fall beklagten sich Gemeinderäte, dass ohne ihre Zustimmung zumindest ihre Wortbeiträge im Internetangebot der Gemeinde „live“ zur Verfügung gestellt wurden (Nr. 11.2). In diesem nicht ganz einfach gelagerten Fall bin ich, auch im Hinblick auf die Tatsache, dass der Gemeinderat ein Verwaltungsorgan der Gemeinde ist, zu dem Ergebnis gekommen, dass es der einzelne Teilnehmer trotz der Öffentlichkeit von Gemeinderatssitzungen nicht hinnehmen muss, dass seine Beiträge weltweit speicher- und verarbeitungsfähig im Internet zur Verfügung gestellt werden. Ein zweiter Komplex, der immer wieder angesprochen werden muss, ist die weitere Auswertung von Bürgerdaten, die im Rahmen von Bürgerbegehren oder sonstigen bürgerschaftlichen Engagements anfallen: So wurde ein Bürgerbegehren dahingehend ausgewertet, in welchem Prozentsatz sich bestimmte Altersgruppen an dem Begehren beteiligt haben. Für diese statistisch vielleicht ganz interessante Frage darf ein Bürgermeister die mit der Einreichung des Begehrens verbundenen personenbezogenen Daten aber nicht auswerten, da diese ausschließlich zur Feststellung der Zulässigkeit des Begehrens genutzt werden dürfen. In einem anderen Fall wurden Bürger, die einer Aufforderung zu einer Meldung nicht nachgekommen waren, in einer Ortsteilversammlung namentlich an den Pranger gestellt. Ich erwähne diese Fälle hier, weil ich fast in jedem Tätigkeitsbericht Fälle dieser Art schildern muss. Schließlich habe ich in diesem Berichtszeitraum wieder zahlreiche Beschwerden von Bürgerinnen und Bürgern über die Zusendung von Wahlwerbeschreiben politischer Parteien erhalten. Dies zeigt mir, dass doch viel dafür gesprochen hätte, wie von den Datenschutzbeauftragten gefordert, für die Adressübermittlung an Parteien vor Wahlen die Zustimmung der Betroffenen zu fordern. Immerhin ist jetzt die Pflicht der Meldebehörden eingeführt, acht Monate vor Wahlen die Bürger und Bürgerinnen auf ihr Widerspruchsrecht hinzuweisen. Wenigstens ein Fortschritt.

2.1.5 Gesundheit und Soziales

Neben den oben unter „Schwerpunkten“ aufgeführten Komplexen „Gesundheitskarte“ und „JobCard-Verfahren“ war ich in diesem Bereich mit einer Vielzahl von unterschiedlichsten Fragen befasst, die allerdings eines gemeinsam hatten: Es ging dabei mit Sozial-, Gesundheits- und medizinischen Daten um sehr sensible Fragen. Drei Punkte greife ich heraus:

Zahlreiche Protestschreiben erreichten mich wegen des Datenabgleichs der BAföG-Ämter mit dem Bundesamt für Finanzen. Dieser Abgleich hatte für viele, die ihre Kapitaleinkünfte verschwiegen hatten, mit Rückforderungsbescheiden und strafrechtlichen Ermittlungsverfahren sehr unangenehme Folgen. Ich habe mich trotz rechtlicher Bedenken, wie auch nach meiner Kenntnis die anderen Datenschutzbeauftragten, letztlich nicht gegen den Abgleich gewandt. Datenabgleiche im Einzelfall wären ohne weiteres zulässig gewesen, da zur Aufgabenerfüllung der BAföG-Ämter erforderlich. Die komplette Überprüfung habe ich für eine Übergangszeit nur im Hinblick auf die dargelegten großflächigen Missbräuche hingenommen. Die Bundesregierung hat inzwischen eine klarstellende Ergänzung des BAföG vorgelegt (Nr. 6.3).

Ein Problem, das auch jetzt im Zusammenhang mit den umfangreichen Fragebögen zur Gewährung des Arbeitslosengeld II für großen Unmut gesorgt hat, wurde auch an mich herangetragen: Bei der Gestaltung von Fragebögen wird zu wenig darauf geachtet, ob durch sie sensible Angaben an Dritte übermittelt werden. Das amtliche Formular Verdienstbescheinigung für einen Antrag auf Wohngeld enthielt die Angabe „für Wohngeld“ und damit die Mitteilung an den Arbeitgeber, dass der Betreffende Wohngeld bezieht. Das bundesweit verwendete Formular wurde auf Grund meiner Initiative inzwischen neutral gefasst (Nr. 6.4).

Für das Programm „Mammographie-Screening“ musste ich datenschutzrechtliches Neuland betreten. Dieses Programm ist ein Angebot an alle Frauen zwischen 50 und 69 Jahren, sich auf Brustkrebs un-

tersuchen zu lassen. Für das Einladungswesen, die Speicherung der Untersuchungsergebnisse in einer Screening-Datenbank und den Abgleich der Ergebnisse mit den klinischen Krebsregistern waren und sind komplexe datenschutzrechtliche Fragen zu lösen. Die Rechtsgrundlage für die Übermittlung von Meldedaten an die Einladungsstelle ist zu schaffen, dies geschieht zur Zeit. Die Information der teilnehmenden Frauen über das Verfahren muss richtig, vollständig und dabei verständlich sein. Dies stellte hohe Anforderungen an die Gestaltung des Informationsmaterials. Für die Evaluation des Screenings ist ein pseudonymisierter Abgleich mit klinischen Krebsregistern erforderlich. Dies ist mit Einwilligung der betroffenen Frau möglich, gleichwohl wird auch insoweit geprüft, ob das Aufgabenspektrum der klinischen Krebsregister insoweit zu ergänzen ist. Im Hinblick auf die umfassende Aufklärung der betroffenen Frauen und ihre freie Entscheidung, an dem Verfahren teilzunehmen, dränge ich zwar auf die Lösung der offenen, mehr verfahrensrechtlichen Fragen, habe aber den Start des Programms nicht blockiert (Nr. 6.2).

2.1.6 Schulen und Hochschulen

Drei Beiträge von allgemeiner Bedeutung bzw. als immer wiederkehrende Fragestellungen seien hier zunächst hervorgehoben: Eine Fachschule hatte ohne Einwilligung ihrer Schüler Zensuren und Abschlusszeugnisse an eine Firma weitergeleitet, bei der die Schüler tätig waren. Die Schüler hatten sich zwar gegenüber der Firma verpflichtet, jederzeit über ihren Ausbildungsstand Auskunft zu geben, nicht aber die Erlaubnis zur unmittelbaren Notenweitergabe erteilt. Deswegen war die Weitergabe der Noten ohne das ausdrückliche schriftliche Einverständnis der Schüler unzulässig (Nr. 20.1.5).

Das Kultusministerium hat vor dem Hintergrund der Tragödie von Erfurt ein Sicherheitskonzept für Schulen entwickelt, bei dessen Erarbeitung es leider versäumt wurde mich einzuschalten. Auf Grund zahlreicher Anfragen zu offenen datenschutzrechtlichen Punkten habe ich mich nachträglich eingeschaltet und zu Fragen der Datenübermittlung, z.B. von Schule an Polizei und der Hinterlegung von Adressen, datenschutzgerechte und praktikable Lösungen erarbeitet. Diese wurden den Schulen vom Kultusministerium nachträglich mit einem Schreiben übermittelt. Unter anderem habe ich gefordert, dass nicht jede Ordnungsmaßnahme der Polizei übermittelt wird und dass Adressdaten der Eltern der Schüler nur in verschlossenem Umschlag bei den zuständigen Stellen hinterlegt werden (Nr. 20.1.2).

Immer wieder werde ich mit der Frage der Veröffentlichung von Schülerfotos befasst. Ich möchte deshalb auch an dieser Stelle darauf hinweisen, dass eine Veröffentlichung von Schülerfotos im Internet nur mit Einwilligung des betroffenen Schülers bzw. der betroffenen Schülerin zulässig ist (Nr. 20.1.3).

Schließlich noch eine Erfolgsmeldung: Im letzten Tätigkeitsbericht hatte ich unter 16.1.1 über die neu eingeführte grundsätzliche Pflicht der Schulen berichtet, die Eltern auch volljähriger Schülerinnen und Schüler von schwer wiegenden Ordnungsmaßnahmen zu unterrichten. Für selbstverständlich hatte ich es gehalten, dass die Schülerinnen und Schüler vorher zu informieren seien. Das Kultusministerium sah dies ursprünglich nicht so. Erst nachdem ich mich persönlich an den Amtschef des Kultusministeriums gewandt hatte, wurde eine solche Informationspflicht angeordnet. Der Bayerische Verfassungsgerichtshof hat nunmehr diese Informationsverpflichtung als wesentlichen Grund für die Verfassungsmäßigkeit der angegriffenen Regelung angesehen (Nr. 20.1.1).

Aus dem Hochschulbereich hebe ich einen Vorgang hervor, der Gelegenheit zu grundsätzlichen Ausführungen zu den Voraussetzungen von Anonymisierung von Daten bei Forschungsvorhaben und einer wirksamen Einwilligungserklärung gegeben hat. Daten sind dann nicht wirksam anonymisiert, wenn auf Grund von genauen Einzelangaben zur Person diese mit vorhandenem oder leicht zu beschaffendem Zusatzwissen identifiziert werden kann. Eine wirksame Einwilligung setzt freie und unbeeinflusste Entscheidungsmöglichkeit voraus, sie muss grundsätzlich schriftlich erfolgen. Anlass dieser Feststellungen war eine Umfrage einer Universität in Schulen zu den Ursachen früher Schwangerschaften. Ich musste die Umfrage beanstanden und die Anonymisierung der Daten durch Herausnahme der identifizierenden Merkmale fordern (Nr. 20.2.2).

2.1.7 Personaldatenschutz und Medien und Telekommunikation

Hier befasste ich mich u.a. mit dem Akteneinsichtsrecht bei Konkurrentenstreitigkeiten, mit der Nutzung von E-Mail am Arbeitsplatz und mit einem Einzelfall, in dem es um Auskunft aus Personalakten und um Löschungs- und Berichtigungsansprüche ging.

Bei Konkurrentenstreitigkeiten besteht grundsätzlich ein Rechtsanspruch des Konkurrenten auf Akteneinsicht in das Protokoll der Vorstellungskommission, nicht dagegen allgemein auf Auskunft aus Personalakten. Derartige Auskünfte sind nur im Einzelfall erst nach sorgfältiger Abwägung der gegenseitigen Interessen zu geben (Nr. 16.1.3).

Häufig gefragt wurde zur privaten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

und inwieweit der Dienstherr bzw. Arbeitgeber dies kontrollieren und protokollieren dürfe. Ich habe auf zahlreiche Veröffentlichungen hingewiesen und ausgeführt, dass grundsätzlich zu unterscheiden ist, ob die private Nutzung erlaubt oder untersagt ist. Soweit die private Nutzung untersagt ist, bestehen weit gehende Kontrollmöglichkeiten. Aber auch hier ist eine automatisierte Vollkontrolle durch den Dienstherrn nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Ist dagegen die private Nutzung erlaubt, gilt der Dienstherr als Telekommunikations- und als Telediensteanbieter und ist deren Pflichten, besonders dem Telekommunikationsgeheimnis, unterworfen. Eine Protokollierung ist nur aus technischen Gründen zulässig, eine Überwachung überhaupt nicht, es sei denn der Betroffene hat in weiter gehende Kontrollmaßnahmen eingewilligt (Nr. 21.1).

Schließlich der Einzelfall, den ich aber wegen seiner allgemeinen Bedeutung hier doch hervorheben möchte: Eine Auseinandersetzung zwischen einer Bediensteten und einer Behörde u.a. über eine Auskunft aus einem Personalaktenverwaltungssystem und über einen Löschungsanspruch eines unrichtigen Datums hat zu erbittertem jahrelangen Schriftwechsel und dicken Aktenbergen geführt. Die Behörde weigerte sich die Ansprüche zu erfüllen, da weitere (wesentliche) Streitpunkte gerichtlich anhängig waren. Ich habe die Behörde beanstandet, da jedenfalls die beiden oben genannten Streitpunkte ohne weiteres auszuräumen gewesen wären: Es ging um einen fehlerhaft eingetragenen Krankheitstag an Christi Himmelfahrt, einem gesetzlichen Feiertag in Bayern. Ich erwähne das hier, weil es mir ein Beispiel dafür ist, wie durch ein frühzeitiges Einräumen eines Mangels jahrelange Streitigkeiten wenn nicht verhindert, so doch zumindest entschärft werden könnten (Nr. 16.1.4).

2.1.8 Technik und Organisation

Der Ausbau des Referates IuK-Technik und -Organisation hat sich als außerordentlich förderlich erwiesen. Durch den Fortschritt in der Informationstechnik sind die Aufgaben dieses Bereichs erheblich angewachsen. Das zeigt sich einmal darin, dass die datenschutzrechtliche Betrachtungsweise in immer größerem Umfang von der informationstechnischen Ausgestaltung der Datenverarbeitungssysteme beeinflusst wird, so dass eine getrennte Aufgabenwahrnehmung des rechtlichen Bereichs einerseits und des technisch-organisatorischen Bereichs andererseits seit langem, in vermehrtem Maße aber in immer größerem Umfang nicht mehr angezeigt, ja nicht mehr möglich ist. Das zeigt sich natürlich auch in dem nach wie vor fast exponenziell steigenden Anwachsen der Informationstechnologien und der Verbreitung informationstechnischer Lösungen im öffentlichen Bereich. Ohne die in den letzten Jahren erreichte personelle Verstärkung der Organisationseinheit IuK-Technik und -Organisation durch junge, engagierte und hoch qualifizierte Mitarbeiterinnen und Mitarbeiter wäre dieser qualitativ geänderte und quantitativ angestiegene Aufgabenbestand nicht angemessen zu bewältigen gewesen. Als sehr förderlich erweist sich auch und gerade in diesem Bereich die Zusammenarbeit im zuständigen Arbeitskreis Technik der Datenschutzkonferenz.

Herausragende Beispiele der notwendigen Integration von rechtlicher Prüfung und informationstechnischer Bewertung sind u.a. die Komplexe Gesundheitskarte, JobCard-Verfahren aber auch die mit der Nutzung der Internettechnologien verbundenen Fragen wie Speicherung von Verkehrs- und Nutzungsdaten und Nutzung von Internetdiensten am Arbeitsplatz. Diese und vergleichbare Themen werden deshalb in enger Kooperation von juristischen und technischen Kolleginnen und Kollegen bearbeitet. Ich möchte deswegen auch an dieser Stelle auf die entsprechenden zusammenfassenden Beiträge im vorhergehenden und auf die detaillierten Ausführungen in diesem Tätigkeitsbericht verweisen.

Neben diesen und anderen Grundsatzthemen hat das technische Referat im Berichtszeitraum die Einhaltung der gebotenen technischen und organisatorischen Datensicherheits- und Datenschutzmaßnahmen in zahlreichen Dienststellen im staatlichen und kommunalen Bereich überprüft. Soweit veranlasst wurde darin auch der Einsatz neuerer Technologien, wie Biometrie zur Zugangskontrolle, Videotechnik und optische Archivierung einbezogen. Die Prüfungsergebnisse zeigen durchweg den Willen zur Beachtung der Anforderungen von Datenschutz und Datensicherheit, mein Referat musste aber feststellen, dass es „doch gelegentlich an einem umfassenden und schlüssigen Sicherheitskonzept bzw. dessen konsequenter Umsetzung“ mangele. Im Einzelnen verweise ich auf die Beiträge unter Nr. 22.2. ff.

In den vergangenen Tätigkeitsberichten hatte ich immer wieder eine kompetente und ressortübergreifende bindende Instanz für die Sicherheit im Bayerischen Behördennetz gefordert. Mit der Zentralen IuK-Leitstelle im Staatsministerium des Innern und mit der führenden Instanz des „Chief Information Security Officer (CISO)“ , dem ein beratendes Sicherheitsteam aus den IT-Sicherheits-Beauftragten der Ministerien und meiner Dienststelle beigegeben ist, steht jetzt eine entsprechende Organisationsstruktur zur Verfügung (Nr. 22.1.1.1). Woran es nach wie vor mangelt, ist die ausreichende elektronische Signatur und Verschlüsselung von E-Mails mit personenbezogenen und sonstigen schutzwürdigen Inhalten im behördlichen Verkehr. Das liegt unter anderem wohl daran, dass die notwendigen Voraussetzun-

gen für den Einsatz des von den zuständigen Gremien ausgewählten Standards S/MIME im Hinblick auf die heterogene Softwarelandschaft in weiten Teilen noch nicht gegeben sind. Dazu zählen auch die notwendigen finanziellen Ressourcen zur Beschaffung der für den Einsatz dieser Software notwendigen Versionen der Betriebssysteme und der Anwendungssoftware. Immerhin bieten inzwischen viele, wenn auch noch nicht alle staatlichen Behörden auf ihren Webseiten PGP-Schlüssel an. Aber auch diese von Betriebssystemen und Anwendungssoftware weitgehend unabhängige und sichere Möglichkeit zur Wahrung der Integrität und Vertraulichkeit wird im innerbehördlichen Verkehr noch nicht ausreichend genutzt.

Abschließend spreche ich das Thema der Auditierung und Zertifizierung von Produkten im Hinblick auf das Einhalten datenschutzrechtlicher Vorgaben an, kurz gesagt das „Gütesiegel für datenschutzfreundliche Produkte“. Dieses Verfahren, das auf sehr positive Resonanz auch seitens der Industrie gestoßen ist, wird mit Erfolg derzeit ausschließlich in Schleswig-Holstein angeboten, das dafür auf Initiative meines dortigen Kollegen Dr. Helmut Bäumler die notwendigen gesetzlichen Grundlagen geschaffen hat. Dieses Verfahren hat sowohl für die Hersteller, die mit sicheren Lösungen werben können, wie für die Verwaltung, deren Prüfungen von zertifizierten Produkten vereinfacht werden, wie für die Bürgerinnen und Bürger, die auf datenschutzgerechte Verarbeitung ihrer persönlichen Informationen vermehrt vertrauen können, ausgesprochene Vorteile. Das Staatsministerium des Innern lehnt dieses Verfahren dagegen ab. Es ist der Auffassung, dass wegen der vorhandenen Datenschutzkontrollinstanzen ein zusätzliches Audit nicht notwendig sei. Durch ein Audit würde neben der Selbstkontrolle durch behördliche und betriebliche Datenschutzbeauftragte und der Fremdkontrolle durch die Datenschutzkontrollbehörden nunmehr eine dreifache Kontrolle eingeführt werden. Dies sei auch angesichts der Kosten nicht vertretbar.

Ich spreche mich wegen der genannten Vorteile gleichwohl dafür aus, dass auch im Bund und in Bayern geprüft wird, ob die gesetzlichen Voraussetzungen für dieses zukunftsorientierte Verfahren geschaffen werden sollen.

2.2 Nationale und internationale Zusammenarbeit der Datenschutzbeauftragten

Diese Zusammenarbeit ist, wie ich auch in den früheren Tätigkeitsberichten bemerkt habe, außerordentlich wichtig. Datenverarbeitung ist länder- und in vermehrtem Maße auch staatenübergreifend. Der regelmäßige Meinungs- und Informationsaustausch ist deshalb unverzichtbar. Das gleiche gilt auch für das Festlegen gemeinsamer Positionen in Entschließungen. Wichtig ist auch das persönliche Kennen. Diesen Zielsetzungen dienen die zweimaligen Treffen auf nationaler Ebene und die jährlichen Treffen der Europäischen Datenschutzbeauftragten sowie die einmal im Jahr stattfindende Internationale Datenschutzkonferenz, an der auch die Datenschutzbeauftragten aus dem außereuropäischen Raum teilnehmen. Ich selbst habe im Berichtszeitraum an den Konferenzen der Datenschutzbeauftragten des Bundes und der Länder sowie an zwei Europäischen Datenschutzkonferenzen teilgenommen. Weiter bin ich Leiter des Arbeitskreises Gesundheit und Soziales und mit meinem Stellvertreter Leiter des Arbeitskreises Justiz der deutschen Datenschutzkonferenz. Die Arbeitskreise tagen regelmäßig zweimal im Jahr, bereiten u.a. Konferenzentschließungen vor und stimmen sich in grundsätzlichen und neu auftretenden Fragen des Datenschutzes ab. Die Zusammenarbeit in diesen Gremien ist aus meiner Sicht sehr gut und für die Arbeit sehr förderlich.

Die Konferenzen der deutschen Datenschutzbeauftragten haben die in der Anlage wiedergegebenen Entschließungen gefasst. Hier hervorheben will ich die Entschließungen zu den Themen Modernisierung des Systems der gesetzlichen Krankenversicherung, Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen, Erweiterung der DNA-Analyse nur mit Augenmaß, zum Gesundheitsmodernisierungsgesetz, zum Entwurf des neuen (inzwischen in Kraft getretenen) Telekommunikationsgesetzes, sowie in der heurigen Frühjahrssitzung zu den Themen Forschungsgeheimnisse für medizinische Daten, Kennzeichen-Scanning durch die Polizei, Übermittlung von Flugpassagierdaten an die US-Behörden, Radio-Frequency Identification (RFID) und schließlich zu den Entscheidungen des Bundesverfassungsgerichts vom 03.03.2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung. Diese Entschließungen wurden den verantwortlichen Ministerien in Bund und Ländern jeweils übermittelt und haben, wenn auch nur zum Teil, Eingang in die weiteren Überlegungen gefunden. Die Themen der beiden Europäischen Datenschutzkonferenzen waren unter anderem Internationaler Datenverkehr und Datenschutzbeschwerden, Datenschutz in der Telekommunikation im Zusammenhang mit der Telekommunikationsrichtlinie, Datenerhebung durch US-Autoritäten im Zusammenhang mit der Bekämpfung des Internationalen Terrorismus.

3 Schlussbemerkung

Ich bin nunmehr im zehnten Jahr meiner Tätigkeit im Datenschutz. Dies hat mich veranlasst, meinen ersten Bericht über das Jahr 1994 nochmals zur Hand zu nehmen. Ein Satz aus meinen damaligen Eingangs-

worten ist zum Motto meiner Tätigkeit und der Datenschutzberichte geworden: Datenschutz ist Grundrechtsschutz. In diesem Sinn gehört der Datenschutzbeauftragte zu den Institutionen, denen ein Wächteramt zum Wohl der Bürgerinnen und Bürger übertragen ist. Ich sehe deshalb meine Aufgabe in erster Linie darin, für datenschutzkonforme und für datenschutzfreundliche Lösungen einzutreten. Das soll mich aber nicht daran hindern darzulegen, welche Verarbeitung personenbezogener Daten zulässig ist, wenn insoweit Zweifelsfragen bestehen. Auch dazu enthält der Tätigkeitsbericht Ausführungen.

In diesem Sinn empfehle ich die folgenden Ausführungen der Aufmerksamkeit der Bürgerinnen und Bürger und der angesprochenen Verwaltungen.

4 Allgemeines Datenschutzrecht

4.1 Freigabepflicht bei der Veröffentlichung von Mitarbeiterdaten im Internet

Der EuGH in Luxemburg hat mit Urteil vom 06.11.2003, Rechtssache C-101/01, entschieden, „dass die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen, erkennbar zu machen, eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten im Sinne von Art. 3 Abs. 1 der EG-Datenschutzrichtlinie darstellt."

Dieses grundlegende Urteil des EuGH hat auch Auswirkungen auf die datenschutzrechtliche Freigabepflicht bei der Veröffentlichung von personenbezogenen Daten im Internet.

Ich habe bisher die Auffassung vertreten, dass das Einstellen eines statischen Datenbestandes - z.B. in Form einer „starren HTML-Seite" - keine automatisierte Verarbeitung darstellt und damit nicht freigabepflichtig ist. Diese Auffassung halte ich angesichts des obigen Urteils nicht mehr aufrecht.

Nach Art. 26 BayDSG bedarf ein automatisiertes Verfahren, mit dem personenbezogene Daten verarbeitet werden, vor dem erstmaligen Einsatz der schriftlichen Freigabe durch den behördlichen Datenschutzbeauftragten und anschließend gemäß Art. 27 BayDSG der Aufnahme in das Verfahrensverzeichnis. Zur datenschutzrechtlichen Freigabe sowie zum Verfahrensverzeichnis habe ich mich bereits in meinem 20. Tätigkeitsbericht unter Nr. 17.1.6 ausführlich geäußert.

Der **Gerichtshof** hat **zur Frage der automatisierten Verarbeitung** ausgeführt, dass es zur Wiedergabe von Informationen auf einer Internetseite nach den gegenwärtig angewandten technischen und EDV-Verfahren eines Hochladens dieser Seite auf einen Server sowie der erforderlichen Vorgänge bedarf, um diese Seite den mit dem Internet verbundenen Personen zugänglich zu machen. Dann hat der Gerichtshof wörtlich festgestellt: „Diese Vorgänge erfolgen zumindest teilweise in automatisierter Form".

In dem vom EuGH beschriebenen Umfang **bedarf deshalb das Einstellen von personenbezogenen Daten in das Internet** - in der Praxis vor allem relevant in Bezug auf Mitarbeiterdaten - **durch bayerische öffentliche Stellen der Freigabe durch den behördlichen Datenschutzbeauftragten** gem. Art. 26 BayDSG. Dies gilt auch, wenn lediglich einmalig ein fest vorgegebener Datenbestand - als so genannte „starre HTML-Seite" - ins Internet eingestellt wird, da das Gericht insofern keine Unterscheidung macht. Das EuGH-Urteil führt damit zu einer Stärkung der Stellung der betroffenen Bürgerinnen und Bürger und mittelbar auch des behördlichen Datenschutzbeauftragten.

Eine Freigabepflicht besteht meiner Auffassung nach allerdings dann nicht, wenn eine Homepage nur solche personenbezogenen Daten enthält, die der „Ersteller" der Web-Site in Vollzug seiner teledienstrechtlichen Pflicht zur Anbieterkennzeichnung - hierzu habe ich mich bereits in meinem 20. Tätigkeitsbericht unter Nr. 17.1.7 ausführlich geäußert - aufgenommen hat. Da gem. § 6 TDG lediglich personenbezogene Daten des Diensteanbieters selbst aufzunehmen sind, sehe ich in einer solchen Fallgestaltung keine Gefährdung des Rechtes auf informationelle Selbstbestimmung, so dass ich auf Grund einer zweckorientierten Beschränkung des Art. 26 Abs. 1 Satz 1 BayDSG keine Freigabepflicht sehe.

Die Frage der Freigabe wird sich bei Internet-Auftritten öffentlicher Stellen immer häufiger stellen. Im Rahmen des ständigen Ausbaus von eGovernment-Lösungen werden immer häufiger auch personenbezogene Daten der wichtigsten Ansprechpartner für den Bürger (etwa Name, akademische Grade, dienstliche Anschrift, dienstliche Telefon- und Faxnummer, dienstliche E-Mail-Adresse, Aufgabenbereich) in das Internet eingestellt. In diesen Fällen greift nunmehr die Freigabepflicht gem. Art. 26 BayDSG ein.

Schließlich möchte ich noch auf Folgendes hinweisen: Im Rahmen des Freigabeverfahrens, aber auch unabhängig davon, ist stets **zu prüfen, ob** die mit einer **Einstellung in das Internet** verbundene Verarbeitung von personenbezogenen Daten nach dem materiellen Datenschutzrecht **inhaltlich zulässig** ist.

Für den Bereich der (kommunalen) Verwaltungen habe ich mich zu dieser Frage bereits im 18. Tätigkeitsbericht unter Nr. 12.3 geäußert. Hinweise für Hochschulen finden sich unter Nr. 16.2.1 meines 20. Tätigkeitsberichts. Vorgaben für die Veröffentlichung von Daten über Lehrer-, Schüler und Elternbeiratsmitglieder im Internet sind in Nr. 15.1 des 18. Tätigkeitsberichts und in Nr. 15.1 des 19. Tätigkeitsberichts enthalten.

4.2 Outsourcing von Verwaltungsleistungen ins Nicht-EU-Ausland

In Anbetracht der aktuellen Reformbestrebungen bin ich in letzter Zeit des öfteren mit der Frage konfrontiert worden, was bei einer Auftragsdatenverarbeitung im Nicht-EU-Ausland von bayerischen Behörden zu beachten ist.

Hierzu gebe ich aus datenschutzrechtlicher Sicht folgende Hinweise:

Bei einem Auftragnehmer aus einem Nicht-EU-Land handelt es sich gem. Art. 4 Abs. 10 Satz 1 BayDSG um einen „Dritten“. Eine Weitergabe von personenbezogenen Daten durch bayerische öffentliche Stellen an einen Dritten stellt somit gem. Art. 4 Abs. 6 Satz 2 Nr. 3 Buchst. a) BayDSG ein „Übermitteln“ dar.

Die Datenübermittlung an Stellen im Ausland ist in Art. 21 BayDSG geregelt. Gemäß den Vorgaben der EG-Datenschutzrichtlinie unterscheidet die Regelung des Art. 21 BayDSG dabei danach, ob das Zielland der EU/dem EWR angehört oder ob es sich um ein sog. „Drittland“ handelt. Nach Art. 21 Abs. 2 Satz 1 BayDSG gilt für die Übermittlung personenbezogener Daten an Stellen in einem sog. „Drittland“ grundsätzlich die Vorschrift des Art. 19 Abs. 1 und 3 BayDSG. In den Fällen der Auftragsdatenverarbeitung kommt in der Regel die Befugnisnorm des Art. 19 Abs. 1 Nr. 1 BayDSG in Betracht. Im konkreten Einzelfall ist vom Auftraggeber sorgfältig zu prüfen, ob die Übermittlung der personenbezogenen Daten an den Auftragnehmer zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Ist dies der Fall, so sind die Voraussetzungen des Art. 19 Abs. 1 Nr. 1 BayDSG i.V.m. Art. 17 Abs. 1 Nr. 2 BayDSG erfüllt, da in den Fällen der Auftragsdatenverarbeitung keine Zweckänderung vorliegt.

Nach Art. 21 Abs. 2 Satz 1 BayDSG ist für die Zulässigkeit der Übermittlung personenbezogener Daten an sog. „Drittländer“ kumulativ erforderlich, dass das „Drittland“ ein **angemessenes Datenschutzniveau** gewährleistet (vgl. Art. 21 Abs. 2 Sätze 2 bis 5 BayDSG). Ob dies der Fall ist, ist von der übermittelnden Behörde eigenständig zu prüfen. Diese schwierige Prüfung ist allerdings dann entbehrlich, wenn die Europäische Kommission förmlich festgestellt hat, dass ein „Drittland“ ein angemessenes Datenschutzniveau gewährleistet (Verfahren gem. Art. 25 Abs. 6 BayDSG i.V.m. Art. 31 Abs. 2 EG-Datenschutzrichtlinie). Eine solche förmliche Feststellung ist bisher beispielsweise in Bezug auf die Schweiz, Ungarn, Guernsey oder Argentinien erfolgt (eine stets aktualisierte Auflistung der „Drittländer“ mit angemessenem Datenschutzniveau findet sich unter http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm#countries).

Allgemein möchte ich noch darauf hinweisen, dass gem. Art. 21 Abs. 3 BayDSG die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle trägt. Nach Art. 6 Abs. 1 Satz 1 BayDSG bleibt der Auftraggeber zudem für die Einhaltung der Vorschriften über den Datenschutz verantwortlich. Der Auftraggeber hat des weiteren die Eignung des Auftragnehmers gem. Art. 6 Abs. 2 Satz 1 BayDSG streng zu prüfen und die Einhaltung der Datensicherheit beim Auftragnehmer gem. Art. 6 Abs. 2 Satz 3 BayDSG zu überwachen. Bei einer Auftragsdatenverarbeitung in „Drittländern“ sind diese Vorschriften über die Verantwortung des Auftraggebers besonders ernst zu nehmen.

4.3 Archivrechtliche Anbietungspflicht und datenschutz-/ disziplinar- und personalaktenrechtliche Löschungspflicht

Im Berichtszeitraum befasste ich mich mehrfach mit dem Verhältnis zwischen archivrechtlicher Anbietungspflicht und datenschutzrechtlicher bzw. disziplinar- und personalaktenrechtlicher Löschungspflicht.

Hier sind zwei Problemkreise zu unterscheiden:

Archivrechtliche Anbietungspflicht und datenschutzrechtliche Löschungspflicht

Solange ein Vorgang noch zur Aufgabenerfüllung der Behörde benötigt wird, steht die spätere archivrechtliche Anbietungspflicht einer aktuellen datenschutzrechtlichen Pflicht, ein einzelnes Datum zu löschen, nicht entgegen.

Im Einzelnen:

Nach Art. 12 Abs. 8 BayDSG ist eine Löschung von personenbezogenen Daten in anbietungspflichtigen Unterlagen erst dann zulässig, wenn das öffentliche Archiv die Unterlagen nicht als archivwürdig übernommen hat oder über die Übernahme nicht fristgerecht entschieden hat. Die Kollisionsregel des Art. 12 Abs. 8 BayDSG sichert so im Ergebnis den Vorrang der in Art. 6 BayArchivG statuierten Anbietungspflicht.

Allerdings kann der Vorrang der archivrechtlichen Anbietungspflicht nur greifen, soweit diese Pflicht tatsächlich reicht: Alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Freistaates Bayern haben gemäß Art. 6 Abs. 1 Satz 1 BayArchivG dem zuständigen staatlichen Archiv die Unterlagen zur Übernahme anzubieten, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen. Gemäß Art. 6 Abs. 1 Satz 2 BayArchivG ist dies in der Regel 30 Jahre nach Entstehung der Unterlagen anzunehmen, soweit durch Rechts- oder Verwaltungsvorschriften der obersten Staatsbehörden nichts anderes bestimmt ist. Werden also die Unterlagen für die Aufgabenerfüllung der Behörde noch benötigt, ist aber ein einzelnes Datum nach Datenschutzrecht zu löschen, greift die Kollisionsregel des Art. 12 Abs. 8 BayDSG nicht ein, da im Zeitpunkt der Anbietungspflicht das Datum nicht mehr existiert. Die (spätere) archivrechtliche Anbietungspflicht steht der (früheren) Löschung der Daten nach Datenschutzrecht also nicht entgegen.

Festzuhalten ist also: Erhebt sich **während der laufenden Bearbeitung des Vorgangs** die Frage, ob Einzeldaten zu löschen sind, ist Prüfungsmaßstab allein Art. 12 BayDSG (und zwar ohne die Vorschrift des Abs. 8). Die Frage der Anbietungspflicht stellt sich nicht.

Wird hingegen die Löschung einzelner Daten eines Vorganges beabsichtigt, der **zur Aufgabenerfüllung der betreffenden Behörde nicht mehr erforderlich** ist, ist zuvor die Frage der Anbietungspflichtigkeit gem. Art. 6 BayArchivG zu prüfen. Besteht diese, ist eine Löschung der Einzeldaten erst unter den Voraussetzungen des Art. 12 Abs. 8 BayDSG zulässig.

Die hier vorgenommene Auslegung wird dem Sinn und Zweck beider Gesetze gerecht: Nur der abgeschlossene Vorgang, nicht aber jedes Einzeldatum soll der Archivverwaltung angeboten werden. An der Anbietung von Einzeldaten besteht seitens der Archivverwaltung auch kein Interesse: diese kann die Archivwürdigkeit nur dann sachgerecht beurteilen, wenn die Unterlagen im Zusammenhang und nach einem gewissen Zeitablauf vorgelegt werden.

Archivrechtliche Anbietungspflicht und disziplinar-/ personalaktenrechtliche Löschungspflicht

Obwohl Disziplinarakten zum Personalakt im materiellen Sinn zählen, weichen u.a. die disziplinarrechtlichen Regelungen des Verwertungsverbots und der Entfernung von Unterlagen vom allgemeinen Personalaktenrecht (Art. 100 ff. BayBG) ab. Demgemäß statuiert Art. 100 f Abs. 1 BayBG den Vorrang der disziplinarrechtlichen Tilgungsvorschrift des Art. 109 BayDO. Nach Art. 109 Abs. 2 Satz 1 BayDO sind die in den Personalakten enthaltenen Eintragungen über die Disziplinarmaßnahmen nach Eintritt des Verwertungsverbots bei Verhängung von Verweis oder Geldbuße auf Antrag des Beamten zu vernichten; in allen anderen Fällen sind sie mit einem entsprechenden Vermerk zu versehen, aus den Personalakten zu entfernen und gesondert aufzubewahren. Diese Vorgänge dürfen nur mit Zustimmung des Beamten eingesehen werden (Art. 109 Abs. 2 Satz 2 BayDO). Disziplinarverfahren, die mit der Verhängung einer schwereren Disziplinarmaßnahme (Versetzung in ein Amt mit geringerem Endgrundgehalt) enden, unterliegen allerdings nicht dem Verwertungsverbot und können auch nicht getilgt werden.

In den Anwendungsbereich des Art. 100 f Abs. 1 BayBG fallen demgegenüber Unterlagen über Beschwerden, Behauptungen und Bewertungen, auf die die Tilgungsvorschriften des Disziplinarrechts keine Anwendung finden, u.a. negative Aussagen über die Leistung oder die Eignung des Beamten. Sie sind nach Nr. 2 dieser Vorschrift auf Antrag des Beamten nach drei Jahren zu entfernen und zu vernichten, falls sie für den Beamten ungünstig sind oder ihm nachteilig werden können. Dies gilt allerdings nicht für dienstliche Beurteilungen.

Nach Art. 11 Abs. 4 Satz 1 BayArchivG sind Unterlagen zu vernichten, wenn sie zum Zeitpunkt der Abgabe an das Archiv von der abgebenden Stelle hätten vernichtet werden müssen. Auf Grund dieser Vorschrift **geht die disziplinar-/personalaktenrechtliche Vernichtungspflicht der archivrechtlichen Anbietungspflicht** vor.

Die „übrigen“ abgeschlossenen - also nicht getilgten - Disziplinarunterlagen, die materiell zum Personalakt gehören, werden gem. Art. 100 g Abs. 4 BayBG nach Ablauf der Aufbewahrungsfrist vernichtet, sofern sie nicht vom zuständigen öffentlichen Archiv nach der in Art. 6 Abs. 1 Satz 1 BayArchivG vorgeschriebenen Anbietung übernommen werden.

5 Gesundheitswesen

5.1 TEMPiS

Die Telemedizin gewinnt im Krankenhausbereich zunehmend an Bedeutung, da sie zur Effizienzsteigerung und Kosteneinsparung im Gesundheitswesen beitragen kann. Telemedizin ermöglicht die Hinzuziehung von Experten, die nicht direkt vor Ort zur Verfügung stehen. Häufig werden somit Verlegungen von Patienten überflüssig, auch wenn das nötige Spezialwissen im behandelnden Krankenhaus selbst nicht vorhanden ist. Ein Beispiel für ein Telemedizin-Projekt, das im Berichtszeitraum von mir beraten wurde, ist das Projekt TEMPiS (Telemedizinisches Pilotprojekt zur integrierten Schlaganfallversorgung in der Region Süd-Ost-Bayern), dessen Projektleitung im Krankenhaus München-Harlaching durchgeführt wird.

Um eine flächendeckend hochqualitative Versorgung von Schlaganfallpatienten zu erreichen, werden derzeit 12 Kooperationskliniken telemedizinisch von zwei Schlaganfallzentren in München-Harlaching und im Universitätsklinikum Regensburg betreut. Dabei können die Kooperationskliniken bei Bedarf 24 Stunden am Tag Schlaganfallpatienten im Schlaganfallzentrum vorstellen. Im ersten Schritt werden hierbei die Computer- und Kernspintomographieaufnahmen des Patienten zur Vorabinformation aus den bildgebenden Systemen des Krankenhauses an das Schlaganfallzentrum übermittelt. Anschließend baut das Schlaganfallzentrum die telemedizinische Verbindung auf, so dass über Bild und Ton eine Kommunikation mit den Ärzten vor Ort und eine Untersuchung des Patienten möglich ist. Dabei ist eine hohe Qualität der Echtzeit-Datenübermittlung nötig, um die Einzelheiten der Patientensymptome zu verfolgen. Nach Abschluss des Konsils wird im Schlaganfallzentrum ein Bericht erstellt und an das behandelnde Krankenhaus übermittelt. Er wird dort in die medizinische Dokumentation des Patienten eingefügt.

Da im Rahmen der Konsile personenbezogene medizinische Daten des Patienten übermittelt und gespeichert werden, sind die üblichen rechtlichen Datenschutzanforderungen zu beachten, die im Kapitel 3.5 meines 19. Tätigkeitsberichts und in Kapitel 3.4 meines 18. Tätigkeitsberichts bereits dargestellt wurden. Grundsätzlich ist das Telekonsil aus juristischer Sicht nicht anders zu behandeln wie eine Beteiligung eines Konsilararztes ohne telemedizinische Unterstützung. Befindet sich der Konsilararzt in einem anderen Krankenhaus, so müssen die datenschutzrechtlichen Vorschriften zur Übermittlung von Patientendaten eingehalten werden. Nach Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz ist eine Übermittlung von Patienten an Dritte insbesondere zulässig im Rahmen des Behandlungsverhältnisses oder wenn die betroffenen Personen eingewilligt haben. Die Übermittlung von Patientendaten an Dritte erfolgt „im Rahmen des Behandlungsverhältnisses“ im vorgenannten Sinne jedenfalls dann, wenn der Patient typischerweise damit rechnen muss, dass ein Konsilararzt hinzugezogen wird. Dies ist etwa der Fall, wenn bereits in der Vergangenheit - zulässigerweise - ein Konsilararzt hinzugezogen wurde. Vorliegend handelt es sich jedoch um ein völlig neu entwickeltes Telekonsilverfahren. Patienten sind mit diesem Verfahren erstmals konfrontiert. Insofern habe ich gefordert, dass sie über das eingesetzte Verfahren aufgeklärt und ihre personenbezogenen Daten nur mit ihrer Einwilligung verarbeitet und genutzt werden. Diese Einwilligung kann auch im Zusammenhang mit dem Behandlungsvertrag abgegeben werden. Sie ist jedoch in diesem Fall im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Eine Besonderheit des Projekts besteht darin, dass bei Schlaganfällen typischerweise ca. 50 % der eingelieferten Patienten nicht mehr einwilligungsfähig sind. Bei diesen wird man mit einer mutmaßlichen Einwilligung arbeiten können. Allerdings sind die Patienten, sobald ihre Einwilligungsfähigkeit wieder hergestellt ist, über die Beteiligung des Schlaganfallzentrums zu informieren.

Weiter sind geeignete technische und organisatorische Maßnahmen zu treffen.

Die technische Ausstattung der Beteiligten im Beispiel TEMPiS besteht für die Telemedizin-Arbeitsplätze in den Schlaganfallzentren aus einem PC mit Lautsprecher und Mikrophon sowie ISDN-Router. In den beteiligten Kliniken wird jeweils ein PC mit Kamera, Mikrophon, Lautsprecher und ISDN-Router eingesetzt. In allen Einrichtungen müssen sich die Telemedizin-Arbeitsplätze in separaten, abschließbaren Räumen befinden, zu denen nur Berechtigte Zutritt haben. Zudem muss die Nutzung der Arbeitsplätze durch ein Passwort (in den Schlaganfallzentren wird für jeden Benutzer ein personenbezogenes Passwort benötigt) geschützt werden, um eine unbefugte Kenntnisnahme der Daten oder einen solchen Verbindungsaufbau zu verhindern. In den teilnehmenden Kliniken sollte immer klar erkennbar sein, wann eine Verbindung besteht. Zur Erhöhung der Sicherheit vor unbefugtem Remote-Zugriff vom Kliniknetz auf die Telemedizin-Arbeitsplätze und umgekehrt bzw. über die externe Verbindung sollten die Arbeitsplätze nicht in das jeweilige Kliniknetz eingebunden werden und höchstens einen Datenimport aus den bildgebenden Systemen nach einem definierten und kontrollierbaren Vorgehen zulassen.

An gespeicherten Daten liegen auf den Arbeitsplätzen vor allem Computer- und Kernspintomographieauf-

nahmen sowie textuelle Befunde, für die angemessene Löschfristen definiert werden müssen. Zur Sicherstellung der Integrität der Daten empfiehlt sich die Verwendung der elektronischen Signatur. Ist dies nicht möglich, kann ein unterschriebener Ausdruck des Befundes als Referenzdokument verwendet werden. Für zukünftige Planungen von Telemedizinprojekten sollte berücksichtigt werden, dass 2006 mit der Einführung der elektronischen Gesundheitskarte die Ärzte eine HPC (Health Professional Card) erhalten (vgl. Nr. 6.1 „Gesundheitsmodernisierungsgesetz und Elektronische Gesundheitskarte“), die u.a. gesetzeskonforme Schlüssel zur elektronischen Signatur enthält.

Um die Vertraulichkeit der Daten während der Übertragung zu sichern, wurde bei TEMPiS von einer Nutzung des Internets abgesehen. Stattdessen werden ISDN-Wählverbindungen mit gebündelten B-Kanälen verwendet, um eine den Qualitätsanforderungen der Bild- und Tonübertragung angemessene Bandbreite zu erhalten. In Falle der Verwendung von ISDN sollten Verbindungen nur von und zu definierten Teilnehmern möglich sein und ISDN-Mechanismen wie geschlossene Benutzergruppen, Rufnummernidentifizierung / Teilnehmer-Authentifizierung oder Callback-Mechanismen genutzt werden. Als weitere Zusatzmaßnahme ist eine verschlüsselte Übertragung zu empfehlen.

Ein weiterer wichtiger Aspekt bei Telemedizin-Projekten ist die Fernwartung, da häufig die technische Ausstattung nicht von der Systemadministration der jeweiligen Krankenhäuser gestellt und betreut wird, sondern von externen Firmen. Es sind daher die in Kapitel 17.1.9 meines 20. Tätigkeitsberichts geforderten Maßnahmen umzusetzen, um eine unbefugte Kenntnisnahme durch die Wartungsfirma zu verhindern.

Für die Revisionsfähigkeit der Datenzugriffe und –übermittlungen ist neben personenbezogenen Kennungen eine Protokollierung sämtlicher datenschutzrelevanten Vorgänge (z.B. Änderungen von Daten und Benutzerrechten, Datenübermittlungen) sowie eine regelmäßige Auswertung und Löschung der Protokolle erforderlich.

5.2 Informationsaustausch zwischen Kliniken für Forensische Psychiatrie und den Bewährungshelfern an den Landgerichten

Im Berichtszeitraum habe ich mich auf Grund einer Anfrage des Verbandes der Bayer. Bezirke mit der Fragestellung befasst, ob und wenn ja unter welchen Voraussetzungen eine forensische Klinik im Laufe der Behandlung eines Maßregelvollzugspatienten patientenbezogene Daten, insbesondere therapeutische Inhalte sowie behandlungs- und entlassungsrelevante Informationen, an die Bewährungshilfe weitergeben darf.

Diesem Anliegen steht die ärztliche Schweigepflicht (vgl. § 203 Abs. 1 Strafgesetzbuch - StGB) entgegen.

Sollen durch eine forensische Klinik eines Bezirkskrankenhauses im Laufe der Behandlung eines Maßregelvollzugspatienten patientenbezogene Daten, therapeutische sowie behandlungs- und entlassungsrelevante Informationen an die Bewährungshilfe weitergegeben werden, so bedarf dies einer **Offenbarungspflicht oder -befugnis im Sinne des § 203 Abs. 1 StGB.** Eine solche dürfte jedoch im Regelfall nicht gegeben sein.

Eine gesetzliche Offenbarungsbefugnis besteht nicht.

Zum einen ergibt sie sich nicht aus dem Bayerischen Krankenhausgesetz, da dieses u.a. für Krankenhäuser im Straf- oder Maßregelvollzug nicht gilt.

Eine gesetzliche Offenbarungsbefugnis folgt auch nicht aus dem Grundsatz der Rechts- und Amtshilfe (Art. 35 Abs. 1 GG). Die Vorschriften der Amtshilfe geben keine Befugnisse, sondern setzen dies voraus.

Schließlich folgt eine Offenbarungsbefugnis auch nicht aus der gesetzlichen Stellung der Bewährungshilfe. Zwar unterstützt der Bewährungshelfer gemäß § 56 d Abs. 3 StGB das nach § 453 b Strafprozessordnung (StPO) zuständige Gericht bei der Überwachung der Lebensführung des Verurteilten. Die für das Gericht geltende Regelung des § 453 b StPO enthält jedoch lediglich eine Aufgabenzuweisung; sie stellt keine selbstständige Rechtsgrundlage für Eingriffe dar. Dem Bewährungshelfer können keine weitergehenden Eingriffsbefugnisse zustehen als dem Gericht, da er diesem unterstellt und ihm gegenüber nach § 56 d Abs. 4 Satz 2 StGB im Rahmen seiner Tätigkeit weisungsgebunden ist.

Eine Offenbarungsbefugnis könnte sich damit nur aus einer Einwilligung des Betroffenen ergeben. Eine solche lag aber nicht vor.

Daher beurteilte ich die Übermittlung von patientenbezogenen Daten an Bewährungshelfer aus Kliniken des Maßregelvollzugs als unzulässig.

5.3 Medizin-Controlling

Mit Beginn des Jahres 2004 fanden gravierende Änderungen in den Abrechnungsgepflogenheiten deutscher Krankenhäuser statt. Es wurde flächendeckend die Fallkostenberechnung auf der Basis von Diagno-

sis Related Groups (DRG) eingeführt. Früher wurde über Tagespflegesätze abgerechnet. Das Entgelt des Krankenhauses bemaß sich im wesentlichen danach, wie viel Zeit ein Patient im Krankenhaus verbracht hat und danach, wie hoch der mit den Krankenkassen vereinbarte Tagespflegesatz war. Für die Abrechnung war in diesem System die Diagnose und die Therapie im Grundsatz unerheblich. Insofern war es in diesem System im Regelfall nicht erforderlich, dass die Krankenhausverwaltung Einblick in Arztbriefe u.ä. nimmt. Dies ändert sich jetzt:

Ab 2004 zahlen die Kassen für Krankenhausaufenthalte jeweils nur noch eine Pauschale. Die Krankenhausverwaltungen müssen dafür zunächst die Diagnosen und Prozeduren exakt und vollständig erfassen. Denn nur so können die DRG´s richtig festgelegt werden. Dafür ist es erforderlich, dass bestimmte Mitarbeiter der Verwaltung, sogenannte Medizin-Controller, Einsicht in die Patientenakten nehmen. Datenschutzrechtlich habe ich diesen Vorgang wie folgt bewertet:

Nach dem Bayerischen Krankenhausgesetz darf die Krankenhausverwaltung Patientendaten nutzen, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich ist. Unter den Begriff der Patientendaten fallen auch die Patientenarztbriefe und die Krankenblätter mit Patientenanamnesen, in denen intime Daten enthalten sind. Diese sind Ausgangspunkt für die richtige Verschlüsselung in DRG´s. Diese Verschlüsselung wird zunächst von Ärzten vorgenommen.

Der Medizincontroller muss Einsicht in die Patientenakten nehmen, um eine exakte und vollständige Erfassung der Diagnosen und der Prozeduren zu gewährleisten. Erste Erfahrungen haben nämlich gezeigt, dass in vielen Fällen eine Ergänzung der vom Arzt erfassten klinischen Dokumentation bzw. der DRG´s durch die Krankenhausverwaltung vorgenommen werden musste. Zwar gibt es auch die Möglichkeit, eine allgemeine Dienstanweisung für Ärzte zu erlassen, in der eine ordentliche Dokumentation vorgeschrieben wird. In der Praxis zeigt sich aber, dass solche Dienstanweisungen nicht immer befolgt werden. Für das Krankenhaus ist es in wirtschaftlicher Hinsicht entscheidend, die Diagnosen und die Prozeduren richtig zu verschlüsseln. Ohne eine Berichtigung müsste das Krankenhaus erhebliche Mindererlöse hinnehmen.

Ich habe daher gegen Medizin-Controller, die in Krankenakten und Ärztebriefe Einsicht nehmen, um die Abrechnung ordnungsgemäß durchzuführen, im Zusammenhang mit einer DRG-Abrechnung keine Einwendungen erhoben.

Die Forderung, dass der Medizincontroller dem ärztlichen Bereich angehören müsste, kennt das Bayerische Krankenhausgesetz nicht. Damit könnten etwa auch Betriebswirte mit medizinischer Zusatzausbildung im Medizincontrolling eingesetzt werden.

6 Sozialbehörden

6.1 Gesundheitsmodernisierungsgesetz und Elektronische Gesundheitskarte

Am 01.01.2004 ist das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz-GMG) vom 14.11.2003 in Kraft getreten. Öffentlich werden vor allen Dingen die Erhöhung der Zuzahlungen und die Streichung von Leistungen diskutiert. Jedoch werden durch das Gesetz auch eine ganze Reihe von datenschutzrechtlichen Fragen aufgeworfen.

Aus Datenschutzsicht äußerst kritisch zu betrachten ist die erweiterte Datenbasis für Krankenkassen. Nach dem neuen § 295 Abs. 2 SGB V sollen nämlich die gesetzlichen Krankenkassen auch die Abrechnungen der niedergelassenen Ärzte über ihre Leistungen „versichertenbezogen“ erhalten. Dies war bislang nicht so. Auch wenn die bisherige Regelung ihre Ursache in erster Linie im gesetzlich garantierten Selbstverwaltungsrecht der Ärzte und der damit verbundenen Rolle der Kassenärztlichen Vereinigung im Rahmen der Abrechnung der Leistungen gehabt haben mag, so hatte die bisherige Regelung doch den datenschutzpolitisch höchst wünschenswerten Effekt, dass die gesetzlichen Krankenkassen in diesem Bereich keine versichertenbezogenen Daten hatten.

Begründet wurde die Novellierung mit einer Änderung im Abrechnungssystem. Während bislang die Krankenkassen an die Kassenärztlichen Vereinigungen eine Gesamtvergütung zu bezahlen hatten, die sich auf der Grundlage einer für jedes Mitglied zu zahlenden Kopfpauschale berechnete, gilt nunmehr die „Gesamtvergütung durch Regelleistungsvolumina“. Die Krankenkassen entrichten an die jeweilige Kassenärztliche Vereinigung mit befreiender Wirkung eine Gesamtvergütung für die gesamte vertragsärztliche Versorgung der Mitglieder. Nach der Gesetzesbegründung wird damit das finanzielle Risiko einer Mengenausweitung der abgerechneten ärztlichen Leistungen auf die Krankenkassen verlagert. Zu Kontrollzwecken müssten die Krankenkassen wesentlich mehr Daten bekommen, als sie bisher erhielten.

Worin liegt nun das datenschutzrechtliche Problem dieser primär gesundheitspolitischen Entscheidung? Es ist zu befürchten, dass die Patienten für die Kran-

kenkassen „gläsern“ werden. Große versichertenbezogene Datenbestände bei den gesetzlichen Krankenkassen wecken Begehrlichkeiten und erhöhen das Missbrauchsrisiko. Insbesondere besteht die Gefahr der Risikoselektion. Denn die gesetzlichen Krankenkassen können nun alle für einen Versicherten erbrachten medizinischen Leistungen - auch über längere Zeiträume hinweg - verknüpfen, prüfen und bewerten. Für den Bürger besteht die Gefahr, dass er aufgrund seiner Erkrankungen als „schlechtes“ Mitglied eingestuft wird. Damit könnten für ihn Nachteile verbunden sein.

Diese Gefahren hätte man dadurch entschärfen können, dass man eine Pseudonymisierung der Daten vorschreibt. Dies hatte in der Tat der Entwurf eines Transparenzgesetzes der gesetzlichen Krankenversicherung vorgesehen. Leider wurden diese Überlegungen nicht realisiert.

Die Gefahr hätte weiter dadurch minimiert werden können, dass das Gesetz angemessen präzise und verbindlich die Grenzen erlaubter Nutzungen festlegt. Aber auch dies ist nicht geschehen, obwohl der Bundesbeauftragte für den Datenschutz unterstützt durch die Landesbeauftragten für den Datenschutz im Gesetzgebungsverfahren auf diesen Punkt hingewiesen hat. Auf der 66. Datenschutzkonferenz in Leipzig haben die Landesbeauftragten für den Datenschutz und der Bundesbeauftragte für den Datenschutz eine Entschließung zum Gesundheitsmodernisierungsgesetz gefasst, in der unter anderem auch dieser Punkt kritisch beleuchtet wurde (siehe Anlage 10).

Ein weiterer wichtiger Punkt des Gesundheitsmodernisierungsgesetzes betrifft die Werbung durch die gesetzlichen Krankenkassen. Die gesetzlichen Krankenkassen stehen untereinander im Wettbewerb. Werbemaßnahmen sind für sie zwingend, wenn sie überleben wollen. Bislang hatte der Gesetzgeber zwar vorgegeben, dass die Krankenkassen im Wettbewerb stünden, er hat jedoch keine Aussagen darüber getroffen, unter welchen Voraussetzungen die Krankenkassen werben dürfen. Dies ist auch ein Problem von datenschutzrechtlicher Bedeutung, da bei jeder personenbezogenen Werbemaßnahme Daten erhoben bzw. genutzt werden. Nunmehr hat der Gesetzgeber in § 284 Abs. 4 SGB V geregelt, dass die Krankenkassen zur Gewinnung von Mitgliedern Daten nur dann erheben, verarbeiten und nutzen dürfen, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Der wichtigste Punkt im Reformvorhaben ist jedoch die elektronische Gesundheitskarte.

Elektronische Gesundheitskarte

Unter diesem Schlagwort findet derzeit ein groß angelegter Wandel im Gesundheitswesen statt. Der technologische Fortschritt in der Computer- und Medizintechnik macht eine Vernetzung aller Beteiligten (z.B. niedergelassene Ärzte, Krankenhäuser, Krankenkassen, Heilberufe, Apotheken) und somit neuartige Anwendungen wie den elektronischen Arztbrief oder die elektronische Patientenakte möglich. Eine Grundidee dieser Neuerungen ist die ständige Verfügbarkeit wichtiger medizinischer Basisdaten eines Patienten - wie z.B. Allergien, schwer wiegende Krankheiten, Arzneimittelunverträglichkeiten - für alle Akteure im Gesundheitswesen, um eine adäquate Behandlung sicherzustellen. Eine weitere Grundidee besteht in der Zusammenführung von Informationen aus bisher getrennten Datenbeständen zu einer integrierten medizinischen Dokumentation, so dass der behandelnde Arzt auch die Vorerkrankungen sowie die Diagnosen und Behandlungen seiner Vorgänger unkompliziert und schnell einsehen kann.

Um derartigen Entwicklungen Rechnung zu tragen, wurden im GMG u.a. im § 291a SGB V entsprechende Grundlagen gesetzlich geregelt. So wird zum 01.01.2006 der Einsatz der Krankenversichertenkarte durch die elektronische Gesundheitskarte erweitert. Diese Karte bietet dann neben den bisherigen Funktionen auch das elektronische Rezept als verpflichtende Anwendung und auf freiwilliger Basis die Anwendungen Notfalldaten, elektronischer Arztbrief, elektronische Patientenakte, Patientenfach und Patientenquittung. Als Ersatz für den Auslandskrankenschein wird ein Sichtausweis aufgebracht. Die Nutzung der neuen Anwendungen soll nur bei Vorlage der Gesundheitskarte durch den Patienten in Verbindung mit einem Heilberufsausweis (HPC, Health Professional Card) des Arztes oder Heilberuflers möglich sein, um die Patientenhoheit zu gewährleisten.

Technische Grundvoraussetzung für die Umsetzung dieser Anwendungen ist, neben der flächendeckenden Einführung der Gesundheitskarte selbst, die Verknüpfung der derzeitigen technischen Insellösungen zu einer gemeinsamen Telematikinfrastruktur für alle Beteiligten, um die Zusammenführung der Daten zu ermöglichen.

Derartige Bestrebungen gibt es nicht nur in Deutschland, sondern europaweit. Eine Vielzahl von Ländern, wie z.B. Frankreich, Österreich, Griechenland, Slowenien und Schweden arbeiten derzeit an der Einführung neuer bzw. der Erweiterung vorhandener Kartensysteme im Gesundheitswesen. Neben dem eigentlichen Zugang zu Leistungen, wie sie die deutsche Krankenversichertenkarte bietet, rücken zuneh-

mend Funktionalitäten wie gesicherte Identifikation, Signatur und Verschlüsselung medizinischer Dokumente, sowie die Bereitstellung von Notfalldaten und Behandlungsinformationen, ins Blickfeld. Zudem wurde im Juni 2004 mit der Einführung der europäischen Health Card begonnen, die im ersten Schritt als Sichtausweis den bisherigen Auslandskrankenschein (E 111) ersetzen soll. Zukünftig ist aber auch hier der EU-weite Zugang zu medizinischen Daten des Patienten geplant.

Datenschutzaspekte der Gesundheitskarte

Das Konzept der elektronischen Gesundheitskarte wirft eine Vielzahl von datenschutzbezogenen Fragen auf, da hier eine neue Qualität des Zugangs und der Nutzung von personenbezogenen medizinischen Daten entsteht. Grundsätzlich muss in allen Fällen sichergestellt werden, dass der Patient die Hoheit über seine Daten behält, d.h. dass er entscheiden kann, welche Daten auf der Gesundheitskarte bzw. in der Telematikinfrastruktur gespeichert werden und wer worauf zugreifen darf.

Zur effektiven Durchsetzung dieser Forderungen muss neben den gesetzlichen Regelungen auch eine angepasste technische Gestaltung der Systeme erfolgen, die Maßnahmen zum Schutz vor unbefugtem Zugriff auf die Daten beinhaltet, gleichzeitig aber auch durch eine gute Handhabbarkeit den Benutzer bei der Wahrnehmung seiner Rechte unterstützt.

Die technischen Details der Gesundheitskarte und Infrastruktur werden derzeit vom BIT4health-Gremium und den Organen der Selbstverwaltung des Gesundheitswesens ausgearbeitet. Einige grundlegende Richtungsentscheidungen, die auch die Vorstellungen des Datenschutzes berücksichtigen, sind jedoch bereits gefallen. Diese umfassen

- die Festlegung der Freiwilligkeit der Anwendungen, bei denen medizinische Daten bereitgestellt werden,
- die Ablehnung einer zentralen Datenspeicherung und
- die Festlegung auf die Patientenhoheit bzgl. der Daten.

An der genauen Umsetzung wird jedoch noch gearbeitet. Um hierauf intensiv Einfluss nehmen zu können, ist seit Mai 2004 eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu diesem Thema tätig, in der ich Mitglied bin. Ziel ist es, die bisher allgemein vorliegenden Anforderungen des Datenschutzes in die Realisierungsdetails einfließen zu lassen.

Von der Arbeitsgruppe wurden u.a. folgende Themen als Schwerpunkte identifiziert, um eine datenschutzfreundliche technische Ausgestaltung zu erreichen:

- Feingranulare Zugriffsrechte und Autorisierung
- Speicherorte der Daten, Betreiberkonzepte
- Schutz der gespeicherten und übertragenen Daten

Zugriffsrechte auf die Gesundheitskarte

Das GMG regelt in § 291 a Abs. 5 Satz 3 SGB V, dass der Zugriff auf bestimmte Daten nur in Verbindung mit einem elektronischen Heilberufsausweis erfolgen darf. Ich halte den Zugriff auf die Daten der Gesundheitskarte nur in Verbindung mit einem elektronischen Heilberufsausweis für eine wesentliche datenschutzrechtliche Errungenschaft des GMG. Denn nur so sind die Versicherten hinreichend davor geschützt, dass auf sie von unbefugten Dritten Druck ausgeübt wird, ihre Gesundheitsdaten zu offenbaren.

Weiter wird aus Datenschutzsicht gefordert, dass der Patient auch differenziert nach einzelnen Angehörigen eines Heilberufs und einzelnen Teilen einer Anwendung über die Einsichtnahme entscheiden können soll. Dies muss technisch im Rahmen des Zugriffs auf die Gesundheitskarte realisiert werden. Zunächst muss sichergestellt werden, dass sich der Heilberufler für jeden Zugriff auf die Gesundheitskarte über seine HPC authentifizieren muss. Für den Einzelzugriff auf Daten müssen weitere Mechanismen zum Freischalten/Sperren durch den Patienten vorhanden sind, z.B. PINs.

Die Umsetzung feingranularer Zugriffsrechte bringt jedoch große technische Schwierigkeiten mit sich, da die Komplexität aufgrund der Anzahl der Beteiligten und der verschiedenen Anwendungen sehr hoch ist. Aus diesem Grunde hat das Bundesministerium für Gesundheit und Soziale Sicherung zur Unterstützung der Einführung der elektronischen Gesundheitskarte am 03.09.2003 ein Konsortium, bestehend aus den Firmen IBM Deutschland GmbH, dem Fraunhofer-Institut für Arbeitswissenschaft und Organisation (IAO), der SAP Deutschland AG & Co KG, der InterComponentWare AG und der ORGA Kartensysteme GmbH, mit einem Projekt namens „bIT4health“beauftragt. Im Mittelpunkt der Arbeiten des Projekts bIT4health steht die Definition einer herstellerneutralen Telematik- Rahmenarchitektur und Sicherheitsinfrastruktur. Weitere begleitende Aktivitäten sind in den Bereichen Akzeptanzbildung, Projektmanagement, Qualitätssicherung und der wissenschaftlichen Begleitung gebündelt. Das Pro-

jektkonsortium »bIT4health« begleitet die Einführung der elektronischen Gesundheitskarte über die Definitionsphase der Rahmenarchitektur hinaus während der Testphase bis hin zur Einführung und dem ersten Betriebsjahr in 2006. Das bIT4health Gremium plant eine zweistufige Umsetzung der Zugriffsrechte: Auf Ebene der Karten soll die Kontrolle der Zugriffe der Benutzergruppen gemäß § 291 a SGB V bezüglich der Anwendung als Ganzes erfolgen. Die weitere Differenzierung der Zugriffe auf einzelne Personen und Teile von Anwendungen soll in den Anwendungsprogrammen stattfinden. Die genaue Ausgestaltung muss jedoch noch spezifiziert werden.

Zusätzlich stellt sich die Frage, in welcher Form der Besitzer der Karte Einsicht in die über ihn gespeicherten Daten nehmen und z.B. Löschungen vornehmen kann. Neben rechtlichen Festlegungen ist hier z.B. eine gesicherte Einsatzumgebung empfehlenswert, die einen Schutz vor unerwünschten Zugriffen sicherstellt und das geforderte Beisein einer HPC Gewähr leistet. Nur so kann garantiert werden, dass sich Gruppen außerhalb des Gesundheitswesens, wie z.B. Arbeitgeber, durch Überredung und Zwang keinen Zugriff auf die Karten von Mitarbeitern verschaffen können. Denkbar wären z.B. Kiosksysteme in den Arztpraxen, an denen der Patient auch ohne direktes Beisein des Arztes tätig werden kann.

Speicherorte, Betreiberkonzept für die Gesundheitskarte

Es besteht Übereinstimmung darüber, dass die medizinischen Daten der Patienten nicht an einer Stelle zusammengeführt werden dürfen, sondern dezentral gespeichert werden. Eine Verknüpfung der Bestände soll nur über die Gesundheitskarte möglich sein. Dabei gibt es jedoch verschiedene Lösungsansätze, die sich in kartenbasierte und serverbasierte unterteilen lassen.

Bei den kartenbasierten Ansätzen sind sämtliche Daten auf der Karte gespeichert und unterliegen damit der alleinigen Obhut des Patienten, bei der serverbasierten Lösung liegen die Daten auf mehreren Servern verteilt. Da aufgrund der Datenmenge nicht für alle Anwendungen ein kartenbasierter Ansatz infrage kommt, ist die Umsetzung von Hybridlösungen zu erwarten. Diese Telematikinfrastruktur wird gemäß dem gesetzlichen Auftrag derzeit von einem Gremium der Selbstverwaltung des Gesundheitswesens (Protego.net) erarbeitet und nach Fertigstellung auch der Arbeitsgruppe zur Bewertung vorgelegt. Da grundsätzlich davon ausgegangen werden kann, dass Daten in vielen Fällen von den erhebenden Stellen (Arztpraxen etc.) nicht 24 Stunden am Tag, 7 Tage die Woche bereitgehalten werden können, sind Lösungen mit Hilfe von Providern, die verteilte Serverkapazitäten zur Verfügung stellen, zu erwarten. Aus Datenschutzsicht ist hierbei besonders darauf zu achten, dass die Provider keine Kenntnis von den auf ihren Systemen gespeicherten Daten nehmen können, z.B. im Rahmen von Wartungsarbeiten.

Schutz der gespeicherten und übertragenen Daten

Die Telematikinfrastruktur muss umfassende technische Sicherheitsmechanismen enthalten, um unbefugte Kenntnisnahme bei der Datenübertragung oder -speicherung zu verhindern. Dies ist ein sehr komplexes Unterfangen, da eine große Anzahl unterschiedlicher Systeme in verschiedenen Verantwortungsbereichen miteinander verknüpft werden muss. Dadurch werden die bisher vorhandenen Insellösungen über andere Netze zugänglich gemacht und unterliegen einem erhöhten Angriffsrisiko. Dennoch muss über geeignete technische Maßnahmen der Schutz aller Systeme, wie z.B. der Praxissysteme der niedergelassenen Ärzte, gewährleistet sein. Es ist daher sinnvoll, nicht nur die technische Integration der Netze voranzutreiben, sondern gleichzeitig eine Definition gemeinsamer Sicherheitsziele, Mindestanforderungen und Maßnahmen vorzunehmen, die anschließend für alle Komponenten verbindlich sind. Der Schwerpunkt aus Datenschutzsicht liegt hierbei auf Maßnahmen, die eine unbefugte Kenntnisnahme oder Veränderung der Daten bei Transport und Speicherung verhindern, wie z.B. Verschlüsselung und Signatur der Daten, Benutzerauthentifizierung über Chipkarten, differenzierte Berechtigungskonzepte etc.

6.2 Mammographie-Screening

In Deutschland erkranken jährlich rund 46 000 Frauen an Brustkrebs. Je früher der Brustkrebs erkannt wird, desto größer sind die Heilungschancen. Um die Qualität in der Brustkrebsfrüherkennung zu verbessern, wurden sowohl auf Bundes- als auch auf Landesebene Programme entwickelt. In Bayern startete am 01.04.2003 das Bayerische Mammographie-Screening-Programm. Alle Frauen in Bayern zwischen 50 und 69 Jahren haben die Möglichkeit daran teilzunehmen. Dabei wird die Einladung zum Bayerischen Mammographie-Screening-Programm von einer Arbeitsgemeinschaft nach § 219 SGB V der gesetzlichen Krankenkassen („Einladungssekretariat“) organisiert. **Für den Zweck der Einladung sowie zur Abrechnung der medizinischen Leistungen werden personenbezogene Daten durch die Arbeitsgemeinschaft auf einer zentral eingerichteten Datenbank der Kassenärztlichen Vereinigung Bayern gespeichert**. Dort wird auch eine Screening-Datenbank unterhalten, in der die Untersuchungsergebnisse des Erst-, des Zweit- und ggf. Drittbefundes verarbeitet werden. Die **Informationen aus der Screening-Datenbank sollen mit dem Bayerischen Klinischen Krebsregister abgeglichen werden**.

Technisch soll das Vorhaben über das KVB Safenet abgewickelt werden (vgl. Nr. 22.2.3.1).

Dieses Programm wirft auch in datenschutzrechtlicher Hinsicht viele Fragen auf. Ich war bereits in einem sehr frühen Stadium in das Projekt eingebunden. Da die Teilnahme am Mammographie-Screening freiwillig ist, ist dafür eine Einwilligung der betroffenen Frauen erforderlich. Diese Einwilligung setzt eine ausreichende Information der betroffenen Frauen voraus. Besonderes Augenmerk habe ich dabei darauf gelegt, dass die betroffenen Frauen über das Verfahren der Datenspeicherungen, -nutzungen und -übermittlungen im ausreichenden Maß aufgeklärt werden. Angesichts der Vielzahl der beteiligten Stellen sind Einwilligung und Information nicht unkompliziert. Ich glaube jedoch, dass in Anbetracht der Komplexität des Projekts eine gute Lösung gefunden wurde.

Mittlerweile hat auch der Bundesausschuss der Ärzte und Krankenkassen Richtlinien für die Einführung des flächendeckenden Mammographie-Screenings auf Bundesebene erarbeitet.

Diese Krebsfrüherkennungsrichtlinien sehen die Einrichtung einer öffentlichen Stelle im Sinne des § 18 Abs. 4 Melderegisterrahmengesetz vor, einer sogenannten „zentralen Stelle“, auf der Grundlage landesrechtlicher Vorschriften. Diese Aufgabe wird in Bayern, wie oben geschildert, vom Einladungssekretariat wahrgenommen. Für die Einladung sind Daten der Melderegister zu verwenden. An die „zentrale Stelle“ sollen Vornamen, Familiennamen, früherer Familienname, einschließlich Geburtsname, Geburtsdatum, Geburtsort und Anschrift übermittelt werden. Die Meldebehörde kann jedoch nicht zwischen privat versicherten und gesetzlich versicherten Frauen differenzieren, sondern soll die Meldedaten aller Frauen im fraglichen Alter übermitteln. Dies ist auch gewollt, da auch privat versicherten Frauen die Möglichkeit der Teilnahme am Mammographie-Screening eröffnet werden soll.

Fraglich ist jedoch die melderechtliche Grundlage für diese Datenübermittlungen. Zwar ist o.g. Arbeitsgemeinschaft nach § 219 Abs. 1 SGB V eine öffentliche Stelle im Sinne des Melderechts. Übermittlungen an öffentliche Stellen sind melderechtlich privilegiert. Der öffentlichen Stelle „Arbeitsgemeinschaft“ sollen jedoch mit der Einladung auch privat Versicherter auch Aufgaben zugewiesen werden, die nichts mit dem System der gesetzlichen Krankenversicherung zu tun haben. Ich habe das Bayerische Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen auf dieses Problem hingewiesen. Da es sich dabei um eine Frage handelt, die sich bundesweit stellt, hat die Bayerische Staatsministerin die Bundesministerin für Gesundheit und Soziale Sicherung gebeten, eine entsprechende Regelung auf Bundesebene zu schaffen. Das Ergebnis dieser Initiative bleibt abzuwarten.

6.3 Datenabgleich der BAföG-Ämter mit dem Bundesamt für Finanzen

Studenten und Studentinnen, die als BAföG-Bezieher Kapitalvermögen über der Freigrenze (in der Regel 5.200,- €) beim Bezug von BAföG nicht angegeben haben, verbringen zur Zeit sorgenreiche Nächte. Denn ein automatisierter Datenabgleich zwischen den BAföG-Ämtern und dem Bundesamt für Finanzen (BfF) hat zahlreiche Missbrauchsfälle aufgedeckt. Eine erhebliche Zahl der BAföG-Empfänger hat zu Unrecht Ausbildungsförderung bezogen, weil sie wahrheitswidrige Angaben gemacht haben. Dies hat zum einen verwaltungsrechtliche Konsequenzen: Die BAföG-Ämter erlassen Rückforderungsbescheide. Viel wichtiger sind für die Betroffenen jedoch die strafrechtlichen Folgen. Neben dem Bußgeldtatbestand des § 58 Abs. 1 Nr. 1 BAföG steht der Straftatbestand des Betrugs (§ 263 StGB) im Raum. Eine strafrechtliche Verurteilung hätte vor allen Dingen in den Studiengängen, in denen die Studenten und Studentinnen auf den öffentlichen Arbeitsmarkt angewiesen sind, wie z.B. bei Lehrkräften, gravierende Konsequenzen. Beispielsweise würde eine Verurteilung wegen Betrugs zu einer Geldstrafe von über 100 Tagessätzen im Führungszeugnis, das vom Bundeszentralregister ausgestellt wird, vermerkt. Eine Anstellung im öffentlichen Dienst dürfte damit zumindest erheblich erschwert werden.

Ich bin diesem Datenabgleich wegen der zahlreichen Missbrauchsfälle trotz Bedenken für eine Übergangszeit nicht entgegengetreten.

Bei der datenschutzrechtlichen Bewertung des Abgleichs sind zwei Übermittlungsvorgänge zu unterscheiden:

Zum einen die Datenübermittlung von den BAföG-Ämtern an das BfF und zum anderen die Übermittlung vom BfF an die BAföG-Ämter.

Die Befugnis für die Rückübermittlung nach erfolgten Abgleich durch das BfF ergibt sich aus § 45 d Abs. 2 Satz 2 EStG. Die Befugnis der Sozialleistungsträger (BAföG-Ämter), die für den Abgleich beim BfF erforderlichen Daten zu übermitteln, ist für den **Einzelfall** aus § 69 Abs. 1 Nr. 1 SGB X herzuleiten. Danach dürfen Sozialdaten übermittelt werden für die Erfüllung der Zwecke einer gesetzlichen Aufgabe der übermittelnden Leistungsträger. Hierzu gehört auch die Überprüfung der Angaben der Leistungsempfänger.

Grundsätzlich sind vollständige Datenabgleiche datenschutzrechtlich nicht unproblematisch. Deshalb gelten für vollständige Datenabgleiche grundsätzlich Sonderregelungen, wie z.B. § 117 BSHG, der den automatisierten Datenabgleich von Sozialhilfeempfängern z.B. mit dem Datenbestand der Bundesagentur für Arbeit oder den Rentenversicherungen zulässt. Maßgebend für eine solche Regelung war die Erkenntnis, dass es zu großen Missbräuchen gekommen ist, denen mit Einzelfallprüfungen nicht mehr effektiv entgegengetreten werden konnte.

Es war deshalb fraglich und unter den Datenschutzbeauftragten auch umstritten, ob man auch den **vollständigen** Datenabgleich auf § 69 Abs. 1 Nr. 1 SGB X stützen kann. Da in der vorliegenden Fallgestaltung bundesweit Leistungsmissbrauch in einem großen Umfang dargelegt wurde und überdies begründet wurde, dass die Durchführung von Stichproben oder die Überprüfung nur in Verdachtsfällen keine entsprechenden Mittel zur Bekämpfung der Missbräuche mehr darstellen, bin ich wegen der gleichen Interessenlage, die zur Schaffung des § 117 BSHG geführt hat, für eine Übergangszeit bis zur Schaffung einer gesetzlichen Regelung einem vollständigen Abgleich nicht entgegengetreten.

Mittlerweile wurde mit den Gesetzgebungsarbeiten zur Schaffung einer (klarstellenden) Regelung für den Datenabgleich im BAföG begonnen.

6.4 Formulare zur Beantragung von Wohngeld

Die Gestaltung von Formularen wirft oft datenschutzrechtliche Probleme auf, die auf den ersten Blick gar nicht erkennbar sind. Denn vielfach geht aus Formularen, die von Dritten auszufüllen sind, direkt oder indirekt hervor, dass der Betreffende auf Sozialleistungen angewiesen ist.

Das stellt eine Übermittlung von Sozialdaten dar, die nicht erforderlich ist. Es muss deswegen darauf geachtet werden, dass der Antragsteller auch neutrale Formulare verwenden kann.

Was ist aber, wenn der Antragsteller behördlicherseits gewissermaßen „gezwungen“ wird, offizielle Formulare zu verwenden, aus denen für den Arbeitgeber unschwer erkennbar ist, dass es sich um einen Bedürftigen handelt? Hier ist es notwendig, das amtliche Formular so zu gestalten, dass die Eigenschaft „Bedürftiger“ nicht erkennbar ist.

Ein entsprechender Fall war mir im Zusammenhang mit der Beantragung von Wohngeld vorgetragen worden:

Ein Petent hat sich gegen das Formblatt „Verdienstbescheinigung“ gewandt, weil daraus hervorgeht, dass es für die Wohngeldbeantragung verwendet wird. Das gemäß AllMBl Nr. 4/2002 S. 165 verwendete Formular ließ erkennen, dass der Antragsteller Wohngeld beantragt. Ich habe die Formulierung im Titel des Formulars „Verdienstbescheinigung zum Antrag auf Wohngeld“ und die Angabe der Wohngeldnummer als für eine nach dem SGB unzulässige, da nicht erforderliche Übermittlung von Sozialdaten an Dritte gerügt.

Zwar werden die Daten nicht von der Wohngeldstelle bekannt gegeben, sondern vom Antragsteller selbst. Da aber der Antragsteller faktisch dazu gezwungen wird, die ihm von der Wohngeldstelle mitgegebenen Formulare zu verwenden, ist der Fall so zu behandeln, als würde die Wohngeldstelle selbst die Bestätigung des Arbeitgebers einholen und damit die auf dem Formular angegebenen Daten übermitteln.

Bei den Angaben handelt es sich um Sozialdaten nach § 67 Abs. 1 Satz 1 SGB X. Die Datenübermittlung an den Arbeitgeber war nicht nach § 69 Abs. 1 Nr. 1 SGB X zulässig, da sie nicht erforderlich war. Die Wohngeldstelle benötigte lediglich die Angaben über den Verdienst, eine Kenntnis des Arbeitgebers, warum diese Angaben benötigt werden, war weder für diesen, noch für die Wohngeldstelle erforderlich.

Das Formular konnte so neutral formuliert werden, dass der Arbeitgeber nicht erkennen konnte, dass der Arbeitnehmer Wohngeld beantragt hat. Ich hatte deshalb das Bayerische Staatsministerium des Innern aufgefordert, die Verdienstbescheinigung zum Antrag auf Wohngeld dahingehend zu ändern, dass sie den Verwendungszweck nicht mehr erkennen lässt. Auf meine Initiative hin hat es das Bayerische Staatsministerium des Innern erreicht, dass die verwendeten Vordrucke für eine Verdienstbescheinigung zum Antrag auf Wohngeld so geändert wurden, dass sie den Verwendungszweck nicht mehr erkennen lassen.

6.5 Gefahren bei der Verwendung eines Telefaxgerätes

In einer Jugendamts-Angelegenheit war die Kontaktaufnahme mit einem Erziehungsberechtigten durch die Behörde notwendig. Vom Erziehungsberechtigten war zuvor ein Fax beim Jugendamt eingegangen. Auf diesem Fax waren auf der Faxleiste die absendende Faxnummer und ein - mit dem Erziehungsberechtigten nicht identischer - Name ersichtlich. Im Briefkopf enthielt das Fax lediglich den Namen, die Adresse, Telefonnummer und E-Mail-Adresse des Erziehungsberechtigten. Da das Jugendamt den Erziehungsberechtigten telefonisch nicht erreichen konnte und auf eine E-Mail keine Reaktion erfolgte, hat es

an die - durch das erhaltene Fax - ersichtliche Nummer ein Fax, namentlich an den Erziehungsberechtigten adressiert, gesendet. Die Behörde ging aufgrund von „Anhaltspunkten“ davon aus, dass es sich dabei um den Faxanschluss der Lebensgefährtin des Erziehungsberechtigten handelt. Tatsächlich war dies jedoch der Faxanschluss des Arbeitgebers einer mit dem Erziehungsberechtigten befreundeten Person.

Ich habe die Übermittlung sensibler Daten an das Faxgerät eines Dritten als unzulässig beurteilt.

Gerade der Faxverkehr gefährdet das Recht auf informationelle Selbstbestimmung in vielfältiger Weise. In vorliegender Fallgestaltung wurde die Faxnummer nicht vom Erziehungsberechtigten angegeben, vielmehr war lediglich ersichtlich, von welchem Faxgerät aus versendet wurde (und dass dort ein anderer Name angegebenen war). Unabhängig von der Frage, ob der Einsatz eines Faxgeräts im Sozial(datenschutz)bereich überhaupt zulässig ist, gab der Fall Anlass zu folgenden grundsätzlichen Erwägungen:

Grundsätzlich hat sich die Behörde, wenn ihr die Adresse des Betroffenen bekannt ist, zunächst an diesen schriftlich per Post zu wenden. Denn dann ist in ausreichendem Maße sichergestellt, dass dieser und nur dieser das behördliche Schreiben erhält. Gibt der Adressat des behördlichen Schreibens selbst eine Faxnummer an und kann die Behörde davon ausgehen, dass der Adressat des Schreibens zugleich Empfänger des Faxes sein wird, so kann die Behörde das Schreiben auch per Fax übermitteln. Hat nun die Behörde, wie im vorliegenden Fall, lediglich die Faxnummer einer dritten Person und aber zugleich die postalische Adresse des Betroffenen, so hat sich die Behörde grundsätzlich per Post an den Adressaten ihres Schreibens zu wenden. Allein daraus, dass der Betroffene eine dritte Person mit dem Absenden eines Faxes beauftragt hat und infolge dessen die Faxnummer des Dritten auf der Faxleiste erscheint, kann nicht geschlossen werden, dass der Betroffene unter eben dieser Faxnummer seinerseits nun wieder Faxe zugesendet bekommen möchte. Dies gilt um so mehr, wenn besonders sensible Daten übermittelt werden sollen. Denn selbst wenn sich die dritte Person und der Betroffene nahe stehen sollten, ist nicht auszuschließen, dass der Betroffene nicht wünscht, dass andere Personen Kenntnis vom Inhalt an ihn gerichteter behördlicher Schreiben erhalten.

Ich habe das Jugendamt auf diese Rechtslage hingewiesen und zur künftigen Beachtung aufgefordert.

6.6 Regelmäßige, anlassunabhängige Übersendung von Sozialhilfebescheiden (Abdrucken) an kreisangehörige Gemeinden und Städte durch einen Landkreis

Ein Landkreis (örtlicher Träger der Sozialhilfe) teilte mir mit, kreisangehörige Gemeinden und Städte erhielten einen Abdruck der Sozialhilfebescheide mit der Bitte, dem Landkreis Änderungen in den „Verhältnissen“ des jeweiligen Hilfeempfängers mitzuteilen (insbesondere Umzüge, Sterbetage, Aufnahme von Personen in die Wohnung des Hilfeempfängers usw.). Der Landkreis berief sich auf Art. 9 AGBSHG und auf die Erforderlichkeit, Überzahlungen zu vermeiden. Er bat um meine Stellungnahme, da eine Gemeinde dieses Vorgehen für datenschutzrechtlich unzulässig hielt.

Die Bedenken der Gemeinde waren richtig. Das Landratsamt hatte keine Rechtsgrundlage für die regelmäßige Übermittlung der Bescheide an die Kommunen.

Die Übersendung von Sozialhilfebescheiden an kreisangehörige Gemeinden/Städte ist eine Übermittlung von Sozialdaten, für die eine gesetzliche Grundlage notwendig wäre. Für eine derartige regelmäßige und anlassunabhängige Datenübermittlung bedürfte es zudem einer gesetzlichen Vorschrift, die gerade diese gestattet.

§ 117 Abs. 3 BSHG, der Regelungen zum anlassunabhängigen (auch automatisierten) Datenabgleich enthält, scheidet als Rechtsgrundlage bereits deswegen aus, da auf dieser Grundlage vom Sozialhilfeträger für eine Überprüfung lediglich die in § 117 Abs. 1 Satz 2 BSHG genannten Daten (u.a. Name, Vorname, Geburtsdatum) an die Gemeinden/Städte übermittelt werden dürften. Die in einem Sozialhilfebescheid genannten Daten, insbesondere über die gewährten Leistungen, gehen jedoch über die in § 117 Abs. 1 Satz 2 BSHG genannten Daten hinaus. Zudem dürften in diesem Rahmen auch nur genau bestimmte Daten durch die Gemeinden/Städte überprüft werden (§ 117 Abs. 3 Satz 4 BSHG). Insoweit nehme ich auch auf meinen 18. Tätigkeitsbericht (Nr. 4.5.2) Bezug. Außerdem müssten die Gemeinden/Städte die vom Sozialhilfeträger erhaltenen Daten im Anschluss unverzüglich löschen (§ 117 Abs. 3 Satz 6 BSHG).

Art. 9 Abs. 1 AGBSHG, nach dem kreisangehörige Gemeinden auf Anforderung der Landkreise bei der Feststellung und Prüfung der für die Gewährung von Sozialhilfe erforderlichen Voraussetzungen „mitwirken“, stellt - nach Systematik und Gesetzgebungsgeschichte/-verlauf - keine Rechtsgrundlage für regelmäßige, anlassunabhängige Übermittlungen/Datenabgleiche dar, da er dafür nicht die notwendigen

Voraussetzungen eines konkreten Befugnisrahmens enthält. Diese Vorschrift stellt eine Aufgabenzuweisungs-, aber keine Befugnisnorm dar, die zu konkreten Rechtseingriffen berechtigen würde. Im übrigen wendet sie sich an die Gemeinden, gibt aber dem Sozialhilfeträger keine Befugnisse.

Auch § 69 Abs. 1 SGB X stellt ebenfalls keine solche Rechtsgrundlage dar. Datenübermittlungen können nach dieser Vorschrift unter den dort genannten Voraussetzungen lediglich in konkreten Fällen aus bestimmten Anlässen erfolgen. Derartige konkrete Anlässe gab es hier gerade nicht.

Die regelmäßige, anlassunabhängige Übersendung von Abdrucken der Sozialhilfebescheide an Gemeinden und Städte war deshalb unzulässig. Ich habe den Landkreis daher aufgefordert, dieses Verfahren einzustellen. Dies ist erfolgt. Datenerhebungen und -übermittlungen können allenfalls im Rahmen des § 117 BSHG oder im anlassbezogenen Fall unter Beachtung der §§ 67 ff. SGB X erfolgen.

Im Übrigen hat derjenige, der Sozialleistungen erhält, gemäß § 60 Abs. 1 Satz 1 Nr. 2 SGB I Änderungen in den Verhältnissen, die für die Leistung erheblich sind oder über die im Zusammenhang mit der Leistung Erklärungen abgegeben worden sind, unverzüglich mitzuteilen.

Spiegelbildlich bedürfte es auch auf Seiten der Gemeinden und Städte einer Rechtsgrundlage dafür, aufgrund regelmäßiger, anlassunabhängiger Übersendung von Abdrucken der Sozialhilfebescheide Daten „auf Vorrat“ zu speichern, fortlaufend auf Veränderungen, etwa hinsichtlich der Aufnahme von weiteren Personen in die Wohnung, zu überprüfen und eingetretene Veränderungen dem Landkreis zu melden. Eine dementsprechende gesetzliche Befugnisnorm gibt es jedoch ebenfalls nicht.

7 Polizei

Meine Tätigkeit im Polizeibereich umfasste insbesondere die Kontrolle von Speicherungen in Dateien, wie z.B. im Kriminalaktennachweis, in der Staatsschutzdatei, der Arbeitsdatei „Kfz-Verschiebung“ sowie in weiteren Dateien, insbesondere in regional geführten GAST-Dateien, und von Datenerhebungsmaßnahmen, wie bspw. erkennungsdienstlichen Behandlungen und Speichelprobenentnahmen zum Zwecke der DNA-Analyse. Die Speicherungen im Zusammenhang mit den Münchner Sicherheitskonferenzen 2002 und 2003, die Durchführung eines DNA-Massenscreenings sowie die Videoüberwachung auf öffentlichen Straßen und Plätzen waren weitere Prüfungsschwerpunkte.

Geprüft habe ich auch wieder Datenübermittlungen der Polizei, z.B. an andere öffentliche Stellen oder an die Presse, Abfragen im polizeilichen Informationssystem durch Polizeibedientete sowie die Auskunftserteilung an Betroffene über polizeiliche Speicherungen.

Neben der Kontrolle von Datenerhebung, -nutzung und -verarbeitung durch die Polizei aufgrund von Bürgereingaben, Pressemitteilungen oder sonstigen Hinweisen habe ich auch wieder mehrere anlassunabhängige Prüfungen beim Landeskriminalamt, bei zwei Präsidien und zwei Direktionen vorgenommen.

Des Weiteren habe ich auch auf die datenschutzkonforme Realisierung von Gesetzen, Richtlinien und Errichtungsanordnungen für Dateien hingewirkt, soweit sie Eingriffe in das informationelle Selbstbestimmungsrecht durch die Polizei zum Gegenstand hatten. In diesem Berichtszeitraum waren die geplanten Befugniserweiterungen im Polizeiaufgabengesetz sowie die Richtlinien für die Führung polizeilicher personenbezogener Sammlungen Schwerpunkte meiner Tätigkeit.

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

Die nachfolgenden Darstellungen sind eine Auswahl meiner Feststellungen im Polizeibereich.

7.1 Kriminalaktennachweis (KAN)

Bereits in meinem 20. Tätigkeitsbericht (vgl. Nr. 6.1) hatte ich von den Verhandlungen mit dem Staatsministerium des Innern zur datenschutzrechtlichen Verbesserung des Verfahrens der personenbezogenen Speicherung von Erkenntnissen aus strafrechtlichen Ermittlungsverfahren insbesondere im Kriminalaktennachweis berichtet. Die auch auf meine Forderungen vom Innenministerium in Aussicht gestellte Neufassung der Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (PpS-Richtlinien) und der Errichtungsanordnung für die Personen- und Fall-Auskunftdatei (EA PFAD) ist leider noch nicht erfolgt. Das Innenministerium hat mir aber - nachdem ich zu dem 1. Entwurf die aus datenschutzrechtlicher Sicht notwendigen Änderungsvorschläge gemacht habe - inzwischen einen geänderten Entwurf vorgelegt. Dieser enthält zwar datenschutzrechtliche Verbesserungen, berücksichtigt aber eine Reihe meiner Forderungen nicht.

Zusammengefasst sind das:

- Die zu geringe Berücksichtigung der Fälle geringerer Bedeutung
- Die Weiterspeicherung im KAN, auch wenn der strafprozessuale Anfangsverdacht vernünftigerweise nicht mehr aufrecht erhalten werden kann
- Keine Speicherung des Verfahrensausgangs im KAN
- Keine abschließende Prüfung der Speicherung nach Abschluss der Ermittlungen

Im Einzelnen:

Wesentlicher Punkt ist nach wie vor die unzureichende Regelung der sog. Fälle von geringerer Bedeutung (Art. 38 Abs. 2 Satz 4 Polizeiaufgabengesetz). Der entsprechenden Einstufung kommt deswegen besondere Bedeutung zu, weil in diesen Fällen nach der gesetzlichen Vorgabe eine kürzere Speicherungsfrist als die vorgesehene Regelfrist festzusetzen ist.

Leider hat das Innenministerium als Regelfälle geringerer Bedeutung bei strafrechtlich relevantem Verhalten neben fahrlässig begangenen Straftaten lediglich bestimmte Privatklagedelikte vorgesehen. Diese Beispiele sind unzureichend. „Fälle geringerer Bedeutung“ sind zumindest alle Fälle leichterer Kriminalität. Das sind solche, die im Höchstmaß mit einer geringen Freiheitsstrafe bedroht sind wie z.B. Erschleichen von Leistungen (Freiheitsstrafe bis zu einem Jahr). Darüber hinaus kommen aber auch weitere Antragsdelikte wie Haus- und Familiendiebstahl, Diebstahl und Unterschlagung geringwertiger Sachen oder unbefugter Gebrauch eines Fahrzeugs als Regelfälle geringerer Bedeutung in Betracht. Gleiches gilt soweit die Staatsanwaltschaft oder das Gericht wegen Geringfügigkeit von der Verfolgung abgesehen haben. Ich hätte es deshalb begrüßt, wenn die Regelbeispiele entsprechend erweitert worden wären.

Auch soweit kein Regelfall vorliegt, kann ein Fall geringerer Bedeutung auch bei anderen Delikten (z.B. Betrug, Körperverletzung) vorliegen, wenn eine Einzelfallprüfung die geringere Bedeutung ergibt (vgl. Nr. 6.1 des 20. Tätigkeitsberichts - 3. Absatz). Dieser Auffassung ist nach Besprechung dieser Frage auch das Innenministerium. Eine überflüssige Erschwernis ist die Forderung des Innenministeriums an den polizeilichen Sachbearbeiter nach einer „strengen“ Prüfung, die zusammen mit der Verpflichtung zur Dokumentation der für die Fristverkürzung maßgeblichen Gründe, in der Praxis eine restriktive und damit nicht gesetzeskonforme Prüfungspraxis befürchten lässt.

Leider sind die geltenden PpS-Richtlinien in diesem Bereich auch insoweit unvollständig, als sie eine verkürzte Frist bei Fällen von geringerer Bedeutung lediglich für Erwachsene festlegen. Das Polizeiaufgabengesetz (PAG) sieht eine solche Einschränkung aber nicht vor. Es ist deshalb notwendig, in diesen Fällen eine Verkürzung der Speicherfristen auch für Kinder und Jugendliche vorzusehen, wobei ausgehend von der gesetzlichen Regelfrist verkürzte Speicherungsfristen für Kinder von höchstens einem Jahr und für Jugendliche von höchstens 3 Jahren vorgesehen werden sollten. Der geänderte Entwurf der PpS-Richtlinien sieht nunmehr auch in diesen Fällen eine Verkürzung vor, ohne allerdings die geforderten Regelfristen vorzugeben.

Darüber hinaus sollte eine Speicherung nicht nur dann gelöscht werden, wenn sich aus der Entscheidung der Justiz **eindeutig** ergibt, dass **jeglicher** Tatverdacht entfallen ist, sondern - entsprechend der Regelung im Polizeiaufgabengesetz - wenn der strafprozessuale Anfangsverdacht, der zur Aufnahme in den KAN geführt hat, vernünftigerweise nicht mehr aufrecht erhalten werden kann. Hier zeigt sich erneut die Tendenz des Innenministeriums, den gesetzlichen Schutz des Betroffenen durch polizeiinterne Vorschriften einzuschränken. Des Weiteren halte ich die Streichung einer Regelung für geboten, wonach Verfahrungseinstellungen wie beispielsweise solche nach § 153 StPO oder §§ 45, 47 JGG, bei denen die Schuld des Täters von der Staatsanwaltschaft oder dem Gericht als gering anzusehen und deshalb keine öffentliche Interessen an der Verfolgung gesehen wird, keine Auswirkungen auf die Speicherfristen haben sollen. Gerade in diesen Fällen halte ich eine Prüfung für notwendig, ob eine Verkürzung der Speicherfrist vorzunehmen ist.

Ich werde gegenüber dem Staatsministerium des Innen erneut auf eine Umsetzung meiner Forderungen dringen.

Bei meinen datenschutzrechtlichen Prüfungen habe ich wiederholt festgestellt, dass häufig (unzulässigerweise) nur die Speicherungen im elektronischen Kriminalaktennachweis als Grundlage für die Datenübermittlungen, z.B. an andere Polizeidienststellen, herangezogen wurden. Dort ist die Speicherung des Verfahrensausgangs nicht vorgesehen, so dass dieser auch nicht übermittelt wurde. Datenschutzrechtlich ist es aber durchaus von Bedeutung, dass die Tatsache eines Freispruchs oder einer Verfahrenseinstellung wegen des Fehlens eines hinreichenden Tatverdachts zum jeweiligen Verfahren gespeichert und bei der polizeilichen Nutzung der Speicherung mit berücksichtigt wird. Während bei der Datenübermittlung der Verfahrensausgang regelmäßig aus der Kriminalakte ersehen werden kann, ist dies z.B. bei einem Datenabgleich nach Art. 43 PAG zur Unter-

stützung von Personenkontrollen vor Ort nicht möglich. Ich halte es deshalb für erforderlich, im KAN (aber auch in der polizeilichen Vorgangsverwaltung) den Ausgang des Verfahrens zu dokumentieren.

Das Innenministerium sieht dagegen keine datenschutzrechtliche Notwendigkeit, den Verfahrensausgang zu speichern. Die Information über den Verfahrensausgang sei für die polizeiliche Aufgabenerfüllung - jedenfalls im Rahmen des Kriminalaktenachweises und in der Vorgangsverwaltung - ohne Belang. Soweit ein polizeiliches Informationsinteresse an dieser Erkenntnis besteht, sei sie der Akte bzw. dem Vorgang zu entnehmen.

Ich bedauere diese Haltung des Ministeriums, die die Belastung des Betroffenen durch die unvollständige Speicherung und die polizeiliche Praxis nicht berücksichtigt.

Auch einer weiteren Forderung, die ich bereits in meinem 20. Tätigkeitsbericht dargestellt hatte, will das Innenministerium nicht nachkommen. Danach sollte die Polizei nach Abschluss der Ermittlungen grundsätzlich eine Prüfung durchführen, ob die Speicherung unter Berücksichtigung des Ermittlungsergebnisses weiter zur polizeilichen Aufgabenerfüllung erforderlich ist (vgl. Nr. 6.1 - 4. Absatz). Das Staatsministerium des Innern führt dazu aus, dass die Frage des „ob“ in jeder Phase der Ermittlungen zu prüfen sei. Dies sollte aber in den PpS-Richtlinien ausdrücklich betont werden. Die Notwendigkeit einer solchen Prüfung macht folgendes Beispiel deutlich: Ein Bürger hatte sich an mich gewandt, da er von Zivilbeamten der Polizei kontrolliert worden war. Nach einer Datenabfrage über Polizeifunk war er vor den Augen seines Arbeitgebers durchsucht worden. Bei meiner Prüfung der zur Person des Betroffenen bestehenden Speicherung im Kriminalaktennachweis stellte sich heraus, dass er von der Polizei verdächtigt wurde, als Türsteher einer Diskothek an einer Schlägerei beteiligt gewesen zu sein. Im Verlauf der Ermittlungen stellte sich aufgrund von Zeugenaussagen heraus, dass der Betroffene als Täter nicht in Betracht kam. Trotzdem wurde die Speicherung von der Polizei nach Abschluss der Ermittlungen wegen der unterlassenen Prüfung nicht gelöscht. Erst auf meine Veranlassung kam auch die Polizei zum Ergebnis, dass die Speicherung zu löschen ist. Bei einer Prüfung nach Abschluss der Ermittlungen unter Abwägung der be- und entlastenden Zeugenaussagen, hätte dieses Ergebnis bereits zu diesem früheren Zeitpunkt ohne mein Eingreifen erzielt werden können.

Auf eine weitere Problematik im Zusammenhang mit der fehlerhaften Bezeichnung von Delikten im KAN wurde ich durch eine andere Eingabe aufmerksam. Der Petent lebte vor einigen Jahren in München und war später ausgewandert. Während seines Aufenthalts in München war wegen des Verdachts der Gefährdung im Straßenverkehr gegen ihn ermittelt worden. Im Rahmen einer Sicherheitsüberprüfung im Einwanderungsland musste er zu seiner Überraschung feststellen, dass ihm Gefährdung des Straßenverkehrs auf Grund Alkoholgenusses vorgehalten wurde. Der betreffenden Ermittlungsakte der Staatsanwaltschaft konnte ich entnehmen, dass der Petent wegen Nötigung und Gefährdung des Straßenverkehrs (ohne Zusatzvermerk) angezeigt worden war. Der Betroffene soll auf der Autobahn mit seinem Pkw einen anderen Verkehrsteilnehmer dadurch genötigt haben, dass er die Überholspur über einen längeren Zeitraum nicht freigab. Ein Zusammenhang mit Alkoholgenuss konnte der Ermittlungsakte nicht entnommen werden.

Die Polizei hat mir auf meine Nachfrage mitgeteilt, dass zum Zeitpunkt der Anzeige das betreffende Delikt mit dem Text „Gefährdung des Straßenverkehrs“ erfasst worden war. Bei einer Umstellung des Straftatenkatalogs sei der ursprüngliche Text durch „Gefährdung des Straßenverkehrs - infolge Alkohol“ ersetzt worden. Entsprechend wurde bei allen anderen „Altfällen“ mit gleichem Speicherungstext verfahren, ohne Rücksicht auf den zu Grunde liegenden Sachverhalt.

Über den Einzelfall hinaus war davon auszugehen, dass weitere Personen im Kriminalaktennachweis auf Grund einer solcher Änderungen im Straftatenkatalog mit dem nicht zutreffenden Zusatz „infolge Alkohol“ gespeichert sind. Ich habe deshalb die Polizei zur Prüfung aufgefordert, wie solche fehlerhaften Speicherungen korrigiert werden können. Darüber hinaus habe ich sie aufgefordert, bei künftigen Änderungen des Straftatkatalogs dafür Sorge zu tragen, dass Speicherungen nur mit zutreffenden Deliktsbezeichnungen angezeigt werden. Inzwischen hat mir die Polizei mitgeteilt, dass alle „Altfälle“ entsprechend korrigiert worden sind.

7.2 Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung (PSV)

Zusammengefasst habe ich hier folgende, teilweise schon in früheren Tätigkeitsberichten angesprochene Mängel festgestellt:

- Überlange Aussonderungsprüffristen
- Erhebliche Erweiterung der Zugriffsberechtigung auf die PSV, dadurch Abbau des Unterschieds zwischen (landesweitem) Kriminalaktennachweis und (regionaler) Sachbearbeitung/(Vorgangsverwaltung)
- kein Hinweis auf richterliche Feststellung der Rechtswidrigkeit einer Maßnahme

- In einem Einzelfall regelwidrige Weiterspeicherung wegen fehlerhaften Löschlaufs

Im Einzelnen:

Die in meinem 20. Tätigkeitsbericht (Nr. 6.2) geschilderte Problematik überlanger Aussonderungsprüffristen für personenbezogene Daten Dritter (z.B. Geschädigte, Anzeigeerstatter, Hinweisgeber) ist leider immer noch nicht gelöst. Zwar hat das Staatsministerium des Innern einer „Entkoppelung" der Speicherfristen für diesen Personenkreis von der Frist für die Aussonderung der Kriminalakten der Täter/Tatverdächtigen insoweit zugestimmt, als eine Verlängerung der Aussonderungsfrist für die Kriminalakte auf Grund weiterer Vorgänge (sog. Mitziehklausel nach Art. 38 Abs. 2 Satz 6 PAG) keine Auswirkung auf die Speicherungsdauer Dritter haben soll. Die Speicherfrist soll aber automatisch um 5 Jahre verlängert werden, wenn eine erneute Sachbearbeitung erfolgt. Dies erscheint mir zu weitgehend. Ich habe deshalb das Innenministerium gebeten, in den PpS-Richtlinien festzulegen, dass eine Verlängerung der Speicherfrist nur in Betracht kommt, wenn der Sachbearbeiter bei einer Wiedereröffnung des Vorgangs nach Prüfung zu dem Ergebnis kommt, dass wegen der erneuten Sachbearbeitung eine Verlängerung der Speicherung der Daten Dritter erforderlich ist. Liegen diese Voraussetzungen nicht vor, sind diese Daten zu löschen. Als Gedächtnisstütze für den Sachbearbeiter sollte ein Hinweis in die Datei auf die notwendige Prüfung der Erforderlichkeit einer Verlängerung der Aussonderungsfrist personenbezogenen Daten Dritter bei Neueröffnung eines „alten" Vorgangs aufgenommen werden. Weder darauf, noch auf den Vorschlag, zumindest in den PpS-Richtlinien eine entsprechende Prüfung bei der Wiedereröffnung von Vorgängen vorzusehen, ist das Innenministerium eingegangen.

Eine datenschutzrechtliche Verschlechterung stellt auch die erhebliche Erweiterung des Zugriffs- und Berechtigungskonzeptes für die Vorgangsverwaltung dar. Wie bereits im 20. Tätigkeitsbericht berichtet, hatte ich mich gegen einen bis dahin nur in den Ballungsraumpräsidien München und Nürnberg möglichen präsidiumsweiten Zugriff auf die PSV gewandt, da damit die Differenzierung zwischen dem bayernweiten Kriminalaktennachweis und der regionalen Vorgangsverwaltung aufgegeben würde. Damit nicht genug, teilte mir das Innenministerium wiederum ohne meine vorherige Beteiligung mit, dass es die Zustimmung für einen landesweiten Zugriff auf die PSV für bestimmte Dienststellen des Landeskriminalamtes erteilt hat. Dem folgte als dritte Erweiterung der Entwurf für einen funktionsbezogenen landesweiten Zugriff einer Vielzahl von Bediensteten der Polizei. Die Auswahl der Funktionen war so umfangreich und unbestimmt, dass nur wenigen ein landesweiter Zugriff vorenthalten würde.

Diesem Zugriffs- und Berechtigungskonzept habe ich nicht zugestimmt, da es auf personenbezogene Daten von nur regionaler Bedeutung einen breiten landesweiten Zugriff zulässt, ohne dass die Erforderlichkeit dafür im Einzelnen dargetan wäre. Dadurch können z.B. Opfer einer Vergewaltigung sowie Zeugen oder Betroffene einer Ordnungswidrigkeit landesweit abgefragt werden. Gleiches gilt für Personen, die in der PSV gespeichert werden, weil sie im Rahmen der Münchener Sicherheitskonferenz 2002 (s.u.) zwar in Gewahrsam genommen wurden, von denen aber weder Straftaten begangen wurden noch Staatsschutzerkenntnisse vorgelegen haben.

Nach Auffassung des Innenministeriums verliere der bisherige Gedanke des Schutzbereichs (Ballungsraumpräsidien, Polizeidirektionen) angesichts der hohen Mobilität der Gesellschaft immer mehr an Bedeutung. Zudem stehe der landesweite Zugriff unter dem Vorbehalt der polizeilichen Erforderlichkeit. Deshalb hat es das Konzept trotz meiner Einwände vorläufig in Kraft gesetzt. Es wird aber die Verbände im Rahmen der Umsetzung ausdrücklich auf die erforderliche Sensibilität bei der Vergabe von landesweiten Zugriffsberechtigungen hinweisen.

Ich beabsichtige, zu gegebener Zeit die Vergabe der Zugriffsberechtigungen und den praktischen Gebrauch des bayernweiten Zugriffs im Einzelnen datenschutzrechtlich zu prüfen.

Ein weiteres Defizit der Vorgangsverwaltung, diesmal inhaltlicher Natur, das bei einem landesweiten Zugriff noch verstärkt wird, habe ich im Rahmen meiner datenschutzrechtlichen Prüfung im Zusammenhang mit der Münchner Sicherheitskonferenz festgestellt. In der Vorgangsverwaltungsdatei waren sechs Personen gespeichert, bei denen die Ingewahrsamnahme durch die Polizei vom Amtsgericht bzw. vom Landgericht für rechtswidrig erklärt worden war. Ein Hinweis auf diese richterliche Entscheidung wurde in der Datei jedoch nicht vermerkt, obwohl ein solcher Hinweis für die Bedeutung der Speicherung und damit für die Belastung der Betroffenen von wesentlicher Bedeutung ist. Im Hinblick auf die Doppelfunktion der PSV als Vorgangsverwaltungs- und als polizeiliche Sachbearbeitungsdatei kann diese Unvollständigkeit unter Umständen auch bei polizeilichen Kontrollen unangenehme Konsequenzen für die Betroffenen haben. Ich habe deshalb die Polizei aufgefordert, die gerichtliche Feststellung der Rechtswidrigkeit der Ingewahrsamnahme in geeigneter Form in der PSV zu vermerken. Das Staatsministerium des Innern habe ich gebeten allgemein festzulegen, dass entsprechende Ergänzungen vorzusehen sind, wenn auf Grund einer justiziellen Ent-

scheidung die Rechtswidrigkeit einer dokumentierten Maßnahme feststeht.

Weder die betreffende Polizeidienststelle noch das Innenministerium haben die Notwendigkeit einer Ergänzung gesehen, da der PSV-Eintrag nur die Vornahme der jeweiligen Maßnahme dokumentiere und diese Dokumentation auch bei der justiziellen Feststellung der Rechtswidrigkeit der Vornahme nicht unrichtig werde. Vor einer Datenübermittlung aus der PSV seien die zu Grunde liegenden Unterlagen beizuziehen, aus denen sich die Entscheidung der Justiz ergebe.

Ich bedaure diese wenig datenschutzfreundliche Haltung. Das Innenministerium stellt hier unrichtigerweise nur auf die Funktion „Vorgangsverwaltung“ ab und verdrängt die zweite Funktion, nämlich Grundlage auch der Sachbearbeitung durch die Polizei. Ich halte deshalb die Umsetzung meiner Forderungen im Hinblick auf die Vollständigkeit und Qualität der Daten und besonders wegen des damit verbundenen „ersten Eindrucks“ von einer gespeicherten Person bei einer polizeilichen Dateiabfrage weiter für notwendig. Dass Speicherungen in der PSV unter Umständen auch negative Auswirkungen für Betroffene haben können, zeigt folgender Vorgang:

Ein Petent hatte sich 2004 bei der Polizei beworben und in diesem Zusammenhang auch einer Überprüfung seiner Person durch einen Abgleich seiner Daten mit polizeilichen Dateien zugestimmt. Zu seiner Überraschung wurde er nach dem Datenabgleich von der Einstellungsberaterin mit zwei Strafverfahren konfrontiert, bei denen gegen ihn als Jugendlicher im Jahre 1990 und 1991 ermittelt wurde. Im Kriminalaktennachweis waren die betreffenden Speicherungen zwar rechtzeitig nach Ablauf der 5-jährigen Regelfrist gelöscht worden. Auf Grund eines Fehlers im Löschlauf waren seine personenbezogene Daten zu diesen Ermittlungsverfahren aber noch in der PSV gespeichert. Nach meiner Intervention sind die Daten gelöscht worden. Sie werden - wie mir die Polizei mitgeteilt hat - das Bewerbungsverfahren auch nicht mehr beeinflussen. Ich habe die Polizei aufgefordert, dem Petenten den Sachstand mitzuteilen, insbesondere auch darauf hinzuweisen, dass er sich im Hinblick auf seine Bewerbung zu den o.g. Verfahren nicht mehr äußern muss.

7.3 Speicherungen in sonstigen Dateien

Anlässlich meiner Prüfungen bei bayerischen Polizeidienststellen habe ich neben Speicherungen im Kriminalaktennachweis und in der Vorgangsverwaltung auch Speicherungen in delikts- und dienststellenspezifischen Dateien überprüft. Im Folgenden habe ich die wichtigsten Ergebnisse dieser Prüfungen zusammengefasst:

Ein Schwerpunkt in diesem Berichtszeitraum war die Prüfung von Speicherungen Betroffener wegen politisch motivierter Vorkommnisse. Neben den Speicherungen im Zusammenhang mit den Münchner Sicherheitskonferenzen 2002 und 2003 waren auch Speicherungen in der bayerischen Staatsschutzdatei SDBY einer Polizeidirektion Gegenstand meiner Prüfung. Die von mir dabei festgestellten Mängel wurden von der Polizei auf meine Forderung hin beseitigt. So waren beispielsweise einzelne Speicherungen, die in der Datei nach Ablauf der Speicherfrist nicht automatisiert, sondern nach der Erstellung von Löschlisten durch den Sachbearbeiter händisch hätten gelöscht werden müssen, nicht fristgerecht gelöscht worden. Zudem waren einige Betroffene, bei denen ich die Vorraussetzungen für die Speicherung in der SDBY nicht gesehen habe, dort aufgenommen worden.

Geprüft habe ich auch die Arbeitsdatei „Kfz-Verschiebung“ (ADKV). Sie soll der repressiven und präventiven Bekämpfung der internationalen Kfz-Verschiebung dienen. Darin sollen Informationen über Sachverhalte im Zusammenhang mit dem Diebstahl von Kraftfahrzeugen oder wesentlichen Teilen davon gespeichert werden, wenn Anhaltspunkte für eine organisierte Begehung oder eine Verschiebung in das Ausland vorhanden sind. Ich habe bezüglich des von der Speicherung betroffenen Personenkreises und der Überprüfungsfristen Korrekturbedarf in der Errichtungsanordnung gesehen. So ist in der Datei beispielsweise für die Speicherung von Beifahrern eine 5-jährige Aussonderungsfrist vorgesehen, ohne dass zwischen Beschuldigten und Nichtbeschuldigten unterschieden wird. Ich habe deshalb das Innenministerium aufgefordert, in der Errichtungsanordnung differenzierte Regelungen festzulegen. Dies hat das Innenministerium in Aussicht gestellt.

Bezüglich einzelner Speicherungen habe ich die Polizei zur Löschung bzw. zur Korrektur der vergebenen Speicherfristen aufgefordert. Beispielsweise wurden die Daten eines amerikanischen Staatsbürgers mit einer Überprüfungsfrist von 5 Jahren gespeichert, weil er einen Pkw angemietet hatte und in Begleitung eines weiteren amerikanischen Staatsbürgers damit nach Tschechien ausreisen wollte, obwohl dies laut Polizeibericht nicht der vertraglichen Vereinbarung mit dem Vermieter entsprach. Tatsächlich war in dem Mietvertrag eine Klausel enthalten, wonach das Fahrzeug nicht in „Eastern Europe“ gefahren werden darf. Der Betroffene gab an, nicht gewusst zu haben, dass die Tschechische Republik in Osteuropa liege. Er habe nur nach Prag fahren wollen. Ich habe die Aussage des Betroffenen durchaus für glaubwürdig gehalten, dass er als 20-jähriger US-Soldat ohne

weiterführende Schulbildung nicht beurteilen könne, ob die tschechische Republik geografisch zu Osteuropa gehöre.

Bei der selben Dienststelle habe ich auch eine Datei geprüft, die die Polizei bei der systematischen Auswertung von Printmedien im Hinblick auf Anlage- und Kreditvermittlungsbetrug unterstützen soll. Dabei sollen Inserenten gespeichert werden, deren Angebote durch Inhalt oder Aufmachung den Schluss auf mögliche Betrugshandlungen zulassen. Auch bei dieser Datei habe ich datenschutzrechtliche Verbesserungen in der Errichtungsanordnung sowie die Löschung einzelner Speicherungen gefordert.

Datenschutzrechtliche Bedenken hatte ich im Einzelfall gegen die von der Polizei gewählte Form der Datenerhebung. Bei zwei Vorgängen waren die Beamten mit einem neutralen Fax an den Inserenten herangetreten, um an Informationen zu gelangen, ohne sich als Polizei erkennen zu geben:

Nach Art. 30 Abs. 3 Satz 1 Polizeiaufgabengesetz sind personenbezogene Daten von der Polizei grundsätzlich offen zu erheben. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar sein soll, ist insbesondere zulässig, wenn die Erfüllung polizeilicher Aufgaben auf andere Weise gefährdet oder erheblich erschwert würde. Der Grundsatz der offenen Datenerhebung darf nicht schon durchbrochen werden, wenn eine verdeckte Datenerhebung für die Polizei einfacher oder für den einzelnen Polizeibeamten bequemer wäre, weil er die Konfrontation mit dem Betroffenen scheut. Die Polizei hatte erklärt, dass in der Regel eine offene Datenerhebung genüge. Im Einzelfall, wenn bereits „konkretere Anhaltspunkte für eine Straftat bestehen“, scheide eine offene Datenerhebung aber aus, da von Personen/Firmen mit Betrugsabsicht nur „bereinigte“ oder gar keine Unterlagen mehr vorgelegt würden, so dass der Zweck der Datenerhebung, nämlich die Gefahrenabwehr und das Erkennen und Verfolgen von Straftaten, nicht mehr zu erreichen wäre. Solche Anhaltspunkte waren aber in beiden Fällen für mich nicht erkennbar.

Bei einer Polizeidirektion habe ich zwei Dateien zur Unterstützung der Bekämpfung der Jugendkriminalität, insbesondere der Gewalt an Schulen, sowie der Straßenkriminalität geprüft. Die dabei in der Datei „Jugendkriminalität“ festgestellten Speicherungen von Schulschwänzern zusammen mit Beschuldigten und Verdächtigen von Straftaten habe ich schon deshalb nicht für zulässig gehalten, weil sie dem Zweck der Datei nicht entsprochen haben. Ich habe darüber hinaus eine sehr niedrige Speicherschwelle festgestellt. So wurde z.B. ein 5-jähriger Junge wegen eines Wohnungsbrandes gespeichert. Die Mutter des Kindes hatte angegeben, dass sie eine brennende Kerze auf ein Sideboard im Flur gestellt habe. Von dort habe der Junge sie offensichtlich ins Kinderzimmer getragen und am Kopfende des Stockbettes unter der Matratze aufgestellt. Auf Grund ihrer Überprüfung ging die Polizei davon aus, dass der Betroffene und sein Bruder „gezündelt“ hatten. Ein 8-jähriger Junge wurde gespeichert, da er mit seiner Schwester auf einer Grasfläche „gezündelt“ und dadurch eine etwa 10 mal 2 Meter große Grasfläche gebrannt hatte. Die Speicherung einer fahrlässigen Brandstiftung begangen durch 5- bzw. 8-jährige Kinder in der Datei „Jugendkriminalität“ halte ich nicht für zulässig. Die Polizeidirektion hat mir zwischenzeitlich mitgeteilt, dass die beiden Dateien nicht mehr weitergeführt und gelöscht werden.

7.4 Speicherungen im Zusammenhang mit den Münchner Sicherheitskonferenzen 2002 und 2003

Schon in meinem 20. Tätigkeitsbericht (vgl. Nr. 6.3) hatte ich von meinen datenschutzrechtlichen Bedenken hinsichtlich des Speicherkonzepts der Polizei im Zusammenhang mit der Sicherheitskonferenz 2002 berichtet. Von mir vorgeschlagene Änderungen des Speicherkonzepts wurden von der Polizei abgelehnt. Ich habe deshalb die Speicherungen vor Ort geprüft und folgende Feststellungen gemacht:

In der Zeit vom 01. bis 03.02.2002 fand in München im Hotel „Bayerischer Hof“ die 38. Konferenz für Sicherheitspolitik (SIKO) statt. Bereits im Vorfeld dieser Veranstaltung zeichnete sich die Mobilisierung eines starken Protestpotenzials, nach polizeilichen Erkenntnissen u.a. auch durch linksextremistische/autonome Kreise ab. Nach Einschätzungen des Verfassungsschutzes und der Polizei war mit ca. 2500 – 3000 gewalttätigen Demonstranten zu rechnen. Das Kreisverwaltungsreferat München hatte auf Antrag der Polizei nach § 15 Abs. 1 Versammlungsgesetz ein Versammlungsverbot erlassen. Dies erstreckte sich auf angemeldete Versammlungen am 01. und 02.02.2002 am Marienplatz sowie jegliche Art von Ersatzveranstaltungen unter freiem Himmel von 01.02.2002, 08.00 Uhr bis einschließlich 03.02.2002, 20.00 Uhr. Dieses Verbot wurde auch vom Bayerischen Verwaltungsgerichtshof am 31.01.2002 bestätigt. Trotzdem wurden Versammlungen durchgeführt. Im Laufe der drei Tage wurden nach Angaben der Polizei insgesamt 816 Personen in Gewahrsam und 67 Personen festgenommen. Die Daten dieser Betroffenen wurden - je nach Kategorie - in unterschiedlichen Dateien (Vorgangsverwaltung, Kriminalaktennachweis, Staatsschutzdatei) gespeichert.

Bei meiner Prüfung habe ich festgestellt, dass Betroffene, die in Gewahrsam genommen worden waren und die eine oder mehrere Ordnungswidrigkeiten begangen hatten, auch dann - wenn auch mit ver-

kürzten Fristen - in der Staatsschutzdatei (SDBY) gespeichert wurden, wenn über sie bis zu diesem Zeitpunkt keinerlei Staatsschutzerkenntnisse vorlagen. Darüber hinaus waren von den weit über 500 Betroffenen dieser Kategorie 457 noch nie zuvor polizeilich in Erscheinung getreten.

Bereits bei der Neufassung der Errichtungsanordnung der Staatsschutzdatei und der damit zusammenhängenden Modifizierung des bundesweiten kriminalpolizeilichen Meldedienstes (KPMD-PMK) hatte ich datenschutzrechtliche Bedenken gegen die erhebliche Erleichterung und die damit verbundene Erweiterung der Speicherungsmöglichkeit von Ordnungswidrigkeiten geltend gemacht (vgl. Nr. 6.7 des 20. Tätigkeitsberichts). Insbesondere durch die Aufnahme der Formulierung „wenn Anhaltspunkte dafür vorliegen, dass die Tat den demokratischen Willensbildungsprozess beeinflussen, der Erreichung oder Verhinderung politischer Ziele dienen soll oder sich gegen die Realisierung politischer Entscheidungen richtet“, ist die Möglichkeit eröffnet worden, sämtliche Ordnungswidrigkeiten in der Staatsschutzdatei zu speichern, soweit Anhaltspunkte für einen politischen Hintergrund vorliegen. Trotz meiner Bedenken war das Innenministerium zu einer Änderung der Errichtungsanordnung, die diese Speicherung ermöglicht, nicht bereit.

Wegen der massenhaften Speicherung von Ordnungswidrigkeiten im Zusammenhang mit der SIKO 2002 in der bayerischen Staatsschutzdatei, bin ich nochmals an das Innenministerium wegen einer Änderung der Errichtungsanordnung und der Löschung der Daten der von der Speicherung Betroffenen herangetreten. Die zum Teil noch sehr jungen Betroffenen wurden nur deswegen mit dem Motiv „Linksextremismus“ in der Staatsschutzdatei erfasst, weil sie an einer Demonstration teilgenommen hatten, die im Vorfeld verboten worden war. Solche Speicherungen bergen die Gefahr, dass junge Menschen, die sich bisher sonst nichts haben zu Schulden kommen lassen, durch die Verarbeitung und Nutzung dieser Daten in großer Zahl in die Nähe des politischen Extremismus gerückt werden und dadurch Schaden erleiden. Die Verhältnismäßigkeit ist hier aus meiner Sicht nicht mehr gewahrt.

Das Innenministerium hat leider erneut eine Änderung der Speicherungsvoraussetzungen in der Errichtungsanordnung u.a. mit der Begründung abgelehnt, dass die Speicherung solcher Ordnungswidrigkeiten unerlässlich für das Erkennen und Abbilden von staatsschutzrelevanten möglichen kriminellen Karrieren sei. Die Speicherung der Betroffenen sei für eine lageorientierte polizeiliche Reaktion bei künftigen ähnlich gelagerten Anlässen erforderlich, die in Anbetracht von Ereignissen in der jüngsten Vergangenheit (z.B. Genf, Genua) durchaus zu erwarten seien. Im Hinblick darauf halte es die Speicherung auch nicht für unverhältnismäßig.

Diese Argumentation räumt meine Bedenken gegen die massenhafte Speicherung junger Leute in der Staatsschutzdatei wegen der bloßen Teilnahme an einer verbotenen Demonstration nicht aus. Etwas anderes gilt auch nicht im Hinblick auf die der Speicherung zugrundeliegenden Erwartung der Polizei, dass sich unter den Betroffenen möglicherweise einzelne befinden, die später in staatsschutzmäßiger Hinsicht (nochmals) in Erscheinung treten werden. Ich sehe deshalb in diesen Speicherungen einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, der auch durch berechtigte Staatsschutzinteressen nicht gerechtfertigt ist.

Im Rahmen der Prüfung der Speicherung von Daten Ingewahrsamgenommener habe ich festgestellt, dass neben Ordnungswidrigkeiten auch der Eintrag „Sonstige polizeiliche Gefahrenabwehr (Nr. 2.2.11 PpS-Richtlinien)“ gespeichert war. Die Voraussetzungen zur Speicherung dieses belastenden Zusatzes liegen nach meiner Auffassung aber grundsätzlich nicht vor, da es an zureichenden tatsächlichen Anhaltspunkten für die Annahme fehlt, dass dieser Zusatz zur Aufklärung oder vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung (Art. 30 Abs. 5 PAG), zur Ergreifung von zur Festnahme gesuchten Personen oder zur Abwehr einer im einzelnen Fall bestehenden erheblichen Gefahr erforderlich ist. Ich habe deshalb die Polizei aufgefordert, diesen Zusatz bei allen Betroffenen sowohl in der PSV und - soweit auch dort erfasst - im KAN zu löschen.

Das Polizei wollte die Speicherung zunächst unter Hinweis auf die Notwendigkeit der Verhinderung schwerer Straftaten wie sie bei vergleichbaren Veranstaltungen in Genua, Seattle oder Davos vorgekommen waren, beibehalten. Sie hat aber nach nochmaligem Vorhalt von mir inzwischen mitgeteilt, dass eine Löschung dieses Eintrags im Kriminalaktennachweis erfolgen werde.

Im Zusammenhang mit der Münchner Sicherheitskonferenz 2002 hatte sich auch ein Jugendlicher an mich gewandt, der von der Polizei in Gewahrsam genommen worden war. Ihm war vorgeworfen worden, trotz Verbotes an einer Versammlung teilgenommen zu haben. Seine personenbezogenen Daten waren wegen dieser Ordnungswidrigkeit von der Polizei in der Staatsschutzdatei und in der PSV gespeichert worden. Die speichernde Polizeidienststelle teilte dem Betroffenen auf Anfrage mit, dass der Kriminalaktennachweis zu seiner Person keine Eintragungen aufweise und „lediglich noch regionale Verwaltungsdaten vorgehalten werden“.

Nach einem erneuten an das Landeskriminalamt (LKA) gerichteten Auskunftsantrag des Petenten wurde ihm von dort mitgeteilt, dass über die Vorgangsverwaltungsdaten hinaus keine Auskünfte erteilt werden. Nachdem der Petent mir dieses Schreiben übermittelt hatte, habe ich mich an das LKA gewandt, um die Auskunftserteilung aus datenschutzrechtlicher Sicht zu prüfen. Das LKA berichtete mir, dass der Betroffene nicht nur in der Vorgangsverwaltung, sondern wegen des selben Sachverhalts auch in der Staatsschutzdatei gespeichert sei. Die Auskunftsverweigerung über diese Speicherung stützte das LKA auf Art. 48 Abs. 2 Nr. 1 PAG, wonach eine Auskunft an den Betroffenen unterbleiben kann, soweit eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei, zu besorgen ist.

Ich habe diese Begründung für eine Ablehnung der Auskunftserteilung im vorliegenden Fall für unzureichend gehalten. Der Petent war zwar in Gewahrsam genommen worden. Er war zu diesem Zeitpunkt aber noch Jugendlicher und vorher strafrechtlich nicht in Erscheinung getreten. Auch in der Staatsschutzdatei waren mit Ausnahme der betreffenden Speicherung keine weiteren Erkenntnisse über ihn gespeichert. Hinweise, dass der Petent als Mitglied der linksextremistischen Szene durch sein Auskunftsersuchen Kenntnis über polizeiliche Maßnahmen oder Dateien erlangen wollte oder das Vorliegen sonstiger Geheimhaltungsgründe, waren nicht erkennbar.

Ich habe deshalb die Polizei gebeten ihr Verhalten zu überprüfen und vollständige Auskunft an den Petenten zu erteilen. Das LKA hat dem Petenten daraufhin vollständige Auskunft über seine gespeicherten Daten erteilt. Die speichernde Polizeidienststelle habe ich darauf hingewiesen, dass die von ihr erteilte Auskunft unrichtig war, da sie unzutreffenderweise den Eindruck vermittelt hatte, dass damit Auskunft über alle in diesem Zusammenhang gespeicherten Daten erteilt worden sei. Für den Wiederholungsfall habe ich eine förmliche Beanstandung angekündigt.

Die Polizei hat mir auf Anfrage mitgeteilt, dass für die Speicherungen im Rahmen der Münchner Sicherheitskonferenz 2003 auf ein Konzept wie im Jahr 2002 verzichtet worden war. Allerdings sind im Jahr 2003 auch weit weniger Betroffene gespeichert worden als im Jahr 2002. Im Zusammenhang mit einer Bürgereingabe habe ich eine Reihe von KAN-Speicherungen wegen „sonstiger polizeilicher Gefahrenabwehr - Nr. 2.2.11 RPpS“ (siehe oben) geprüft. Diese hat die Polizei auch hier auf meine Aufforderung hin gelöscht.

Im Zusammenhang mit der Sicherheitskonferenz 2003 steht auch eine Eingabe einer 17-jährigen Jugendlichen, die sich wegen der datenschutzrechtlichen Prüfung ihrer Speicherungen bei der Polizei an mich gewandt hat. Sie hatte am Marienplatz in München ihre 14-jährige Schwester und deren gleichaltrige Freundin abholen wollen. Durch ein Telefongespräch mit ihrer Schwester hatte sie dann erfahren, dass beide hinter dem Rathaus im Zusammenhang mit der zu diesem Zeitpunkt stattfindenden Sicherheitskonferenz vorläufig festgenommen worden waren. Daraufhin war die Petentin zur Gefangenensammelstelle der Polizei hinter dem Rathaus gegangen, um persönlich Kontakt mit ihrer Schwester aufzunehmen. Nach den Stellungnahmen von Polizeibeamten habe sie versucht, die Personalienaufnahme bei den beiden Betroffenen zu stören. Nachdem sie deshalb des Platzes verwiesen worden war, beleidigte sie die Polizeibeamten. Aufgrund dieser Beleidigung wurde sie vorläufig festgenommen, wobei sie nach Angaben der Polizeibeamten, insbesondere durch Stemmen beider Beine gegen den Boden bzw. den Versuch, sich zu Boden fallen zu lassen, Widerstand geleistet habe. Anschließend wurde sie auf der Polizeidienststelle einer erkennungsdienstlichen Behandlung (Foto, Fingerabdrücke) unterzogen.

Die Polizei hat mir aufgrund meiner Zweifel an der Zulässigkeit der erkennungsdienstlichen Behandlung mitgeteilt, dass eine spätere Überprüfung des Sachverhalts ergeben habe, dass die Voraussetzungen für diese Maßnahme nicht vorgelegen haben. Von einer förmlichen Beanstandung habe ich in diesem Fall aber abgesehen, da die erkennungsdienstlichen Unterlagen vernichtet und die polizeilichen Speicherungen dazu gelöscht wurden.

Darüber hinaus war die Petentin wegen dieses Vorgangs auch in der Staatsschutzdatei SDBY gespeichert worden, obwohl diese bisher weder polizeilich, vor allem aber nicht in staatsschutzmäßiger Hinsicht in Erscheinung getreten war. Bei den der Petentin zur Last gelegten Straftaten handelt es sich weder um sog. Staatsschutzdelikte noch um politisch motivierten Straftaten. Die Petentin wollte Kontakt zu ihrer vorläufig festgenommenen Schwester aufnehmen , was ihr durch die Polizei verwehrt wurde. Offensichtlich aus Verärgerung darüber kam es zu der Beleidigung und in der Folge zu dem Versuch, sich der Festnahme zu entziehen. Ein Grund, eine unbelastete 17-Jährige deswegen landesweit in der Staatsschutzdatei zu speichern, ist dies aber nicht. Die Polizei ist erfreulicherweise meiner Aufforderung, diese Speicherung aus der SDBY zu löschen, nachgekommen.

7.5 INPOL-neu

In meinem 19. Tätigkeitsbericht (vgl. Nr. 5.5.1) habe ich von der Neukonzeption des bundesweiten polizeilichen Informationssystems INPOL berichtet.

Inzwischen arbeiten seit dem 16.08.2003 die Polizeien des Bundes und der Länder mit dem neuen Auskunfts- und Fahndungssystem (INPOL-neu). Bis zur Abschaltung des aktuellen INPOL-Systems wird INPOL-neu parallel dazu betrieben. Das neue Verfahren wurde zwar auf Bundesebene entwickelt, die Verantwortung für den Einsatz des Verfahrens in den Ländern und die Zulässigkeit der damit zusammenhängenden Speicherungen „ihrer" Daten tragen aber die Länder selbst.

Der Schwerpunkt bei der Umstellung liegt in der jetzt eingesetzten ersten Ausbaustufe von INPOL-neu im Wesentlichen im technischen Bereich. Neuerungen mit datenschutzrechtlicher Relevanz sind insbesondere die Aufnahme digitalisierter Lichtbilder und die Möglichkeit der zusätzlichen Speicherung sog. Fallgrunddaten, d.h. Daten, die nähere Angaben zum gespeicherten Vorgang enthalten.

Nach Angaben des BKA sind weitere Ausbauschritte des Systems geplant. So soll nach dem mir vorliegenden geänderten Entwurf einer Errichtungsanordnung im Bundes-Kriminalaktennachweis eine Speicherung auch solcher Daten möglich werden, die die bisherigen Zugangskriterien des Bundes-KAN (z.B. Verbrechen oder Straftaten mit überregionaler Bedeutung) nicht erfüllen. Dies kann z.B. der Fall sein, wenn eine der Straftaten die Erheblichkeitsschwelle für Speicherungen im Bundes-KAN überschreitet und eine Prognose ergibt, dass die weiteren Speicherungen zur Verhütung von Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung beitragen können. Ich habe das Innenministerium darauf hingewiesen, dass ich die geplante Erweiterung für zu weit gehend halte, da sie auf Grund der pauschalen Formulierung zu unbestimmt ist und sogar nicht kriminelles Verhalten umfassen könnte.

Im Zusammenhang mit der Änderung der Errichtungsanordnung für den Bundes-KAN steht auch die Möglichkeit der Erfassung eines Hinweises über die zu einer Person durchgeführte DNA-Analyse im Bundes- und Landes-KAN. Eine solche Maßnahme zur vorbeugenden Kriminalitätsbekämpfung hat u.a. zur Voraussetzung, dass Grund zur Annahme besteht, dass gegen den Betroffenen künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung oder gegen die sexuelle Selbstbestimmung zu führen sind. Dadurch ist für den Betroffenen im Hinblick auf die Möglichkeit der Abfrage durch jeden Polizeibeamten im Alltagsbetrieb (mit evtl. entsprechenden Nebenwirkungen für den Betroffenen) eine stigmatisierende Wirkung zu befürchten, wenn beispielsweise bei Personenkontrollen den abfragenden Beamten angezeigt wird, dass eine DNA-Analyse beim Betroffenen durchgeführt wurde.

7.6 Errichtungsanordnungen für GAST-Dateien

Vom Innenministerium wurde mir der Entwurf einer geänderten Rahmenerrichtungsanordnung zur Stellungnahme übermittelt. Sie gibt für die GAST-Dateien (Dateien zur Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten) den zulässigen Rahmen vor, u.a. hinsichtlich des betroffenen Personenkreises, der Art und des Umfangs der zu speichernden personenbezogenen Daten sowie der Aussonderungsprüffristen. Meine datenschutzrechtlichen Forderungen hierzu hat das Innenministerium zum Teil umgesetzt. So wurde insbesondere ein Hinweis auf die Notwendigkeit einer Differenzierung bei der Vergabe der Speicherfristen entsprechend dem jeweils betroffenen Personenkreis in die Errichtungsanordnung aufgenommen.

Von Polizeidienststellen wurden mir wieder zahlreiche Errichtungsanordnungen für neue GAST-Dateien vorgelegt. In diesem Zusammenhang habe ich insbesondere erhebliche Bedenken erhoben wegen der Speicherung von Personen, gegen die sich lediglich ein „polizeilicher Tatverdacht" richtet. Die Speicherungen von Tatverdächtigen richtet sich nach Art. 38 Abs. 2 Satz 1 PAG. Danach kann die Polizei Daten speichern, die sie von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben. Straftatenverdächtig sind Personen, gegen die zumindest ein Anfangsverdacht nach § 152 Strafprozessordnung (StPO) besteht. Ohne einen solchen Anfangsverdacht ist die Speicherung als „Tatverdächtiger" unzulässig. Ein „polizeilicher" Tatverdacht ist weder in der Strafprozessordnung noch im Polizeiaufgabengesetz vorgesehen. Er ist eine polizeiliche (gesetzlich nicht gedeckte) Hilfskonstruktion, um Daten von Personen speichern zu können, zu denen keine tatsächlichen Anhaltspunkte für einen Anfangsverdacht vorliegen, die aber nach polizeilicher Einschätzung als Täter oder Teilnehmer einer Straftat in Betracht kommen können.

Wenn auch eine Speicherung als „Tatverdächtige" ohne Anfangsverdacht grundsätzlich nicht zulässig ist, halte ich eine Speicherung unter anderer Bezeichnung (z.B. Kontaktperson, Gefährder, sonstige Person) für möglich, soweit die Speicherungsvoraussetzungen dafür vorliegen und dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Die Speicherungsdauer ist dabei nach der konkreten Personenkategorie und nach dem Zweck der Datei in der jeweiligen Errichtungsanordnung zu bestimmen. Regelmäßig wird eine Speicherungsdauer von zwei bis fünf Jahren in Betracht kommen.

Das Innenministerium ist nicht bereit, von der Möglichkeit einer Speicherung „polizeilich Tatverdächtiger" Abstand zu nehmen. Es hat allerdings durch die

Änderung der Rahmenerrichtungsanordnung GAST auf die Notwendigkeit der Festsetzung eigenständiger Speicherfristen für „Verdächtige“ hingewiesen. Dies bewirkt - wie die Praxis zeigt - eine regelmäßige Verkürzung der bisher zehnjährigen Speicherfrist auf fünf Jahre. Dies ist zwar einerseits zu begrüßen, andererseits aber wegen des weiteren Festhaltens am „polizeilichen Tatverdacht“ als Speicherungsgrundlage unzureichend. Ich werde deshalb im Einzelnen prüfen, welche Anhaltspunkte für die Speicherung als Tatverdächtiger vorliegen und bei unzureichenden Anhaltspunkten die Löschung bzw. Fristverkürzung fordern.

7.7 Rasterfahndung

In meinem letzten Tätigkeitsbericht (Nr. 6.11) hatte ich über die nach den Terroranschlägen am 11. September 2001 in den USA bundesweit durchgeführten präventiv-polizeilichen Rasterfahndungen zur Enttarnung potenzieller Attentäter (sog. Schläfer) berichtet. In diesem Zusammenhang waren Personendatensätze zu ca. 94.000 Personen an das Landeskriminalamt übermittelt worden, die dem vorgegebenen Profil entsprachen. Diese Daten wurden vom Landeskriminalamt zunächst in der Arbeitsdatei „Rasterfahndung BAO-USA“ gespeichert. Durch einen maschinellen Abgleich dieser Datenbestände wurden sodann ca. 1.900 sog. „Prüffälle“ ermittelt und in der Datei „Terror USA“ gespeichert. Diese Personen sollten näher überprüft werden.

Das Innenministerium und das Landeskriminalamt waren zunächst meiner Forderung nach der Löschung der Datei „Rasterfahndung BAO-USA“ nicht nachgekommen, obwohl der Zweck der Rasterfahndung, nämlich der Abgleich mit den in den Rasterfahndungsanordnungen aufgeführten Daten zur Ermittlung von Trefferfällen, erreicht war. Ich habe meine Forderung nach der Löschung der Daten wiederholt und dabei auch darauf hingewiesen, dass die Arbeitsdatei zur Abarbeitung der Prüffälle nicht erforderlich erscheint und im Hinblick auf die vom Landeskriminalamt vorgenommenen Sperrung der Daten von der Polizei keine aktuelle Erforderlichkeit gesehen wurde.

Im Hinblick darauf, dass das Bundeskriminalamt den Aussonderungstermin für Datensätze aus den Rasterfahndungen der Länder in der dortigen Verbunddatei auf den 31.03.2003 festgelegt hatte, sollte die Arbeitsdatei „Rasterfahndung BAO-USA“ unverzüglich, spätestens jedoch nach diesem Termin, gelöscht werden. Dem ist das Landeskriminalamt schließlich durch Vernichtung der Unterlagen und Datenträger nachgekommen.

Da mir bekannt war, dass die Abarbeitung der sog. Prüffälle zu diesem Zeitpunkt bereits weit fortgeschritten war, habe ich mich mehrfach an das Landeskriminalamt gewandt und um Mitteilung des Sachstands gebeten, um auch eine möglichst frühzeitige Löschung der abgearbeiteten Prüffälle, bei denen sich keine Verdachtsmomente ergeben hatten, sicherzustellen. Eine durch das Landeskriminalamt im Auftrag des Innenministeriums bei den bayerischen Staatsschutzdienststellen durchgeführte Umfrage hierzu ergab, dass auch die Prüffälle mit wenigen Ausnahmen abgeschlossen waren und deshalb ihrer Löschung in der Datei „Terror USA“ zugestimmt werden konnte. Anfang März 2004 teilte mir das Landeskriminalamt schließlich mit, dass die Prüffälle nunmehr gelöscht und die zugehörigen Unterlagen vernichtet worden seien. Damit ist das Thema „Rasterfahndung“ vorerst für mich abgeschlossen.

7.8 Durchführung von DNA-Massenscreening (DNA-Reihenuntersuchung)

Für die Probenentnahme und anschließende DNA-Analyse zum Zwecke der Aufklärung schwerwiegender Straftaten bei einem größeren Kreis von Personen, die nach bestimmen Kriterien ausgewählt wurden, ohne Tatverdächtige oder Beschuldigte zu sein (DNA-Massenscreening), existiert nach zutreffender Ansicht derzeit keine Rechtsgrundlage.

Deshalb werden DNA-Massenscreenings in Bayern auf die Einwilligung des Betroffenen gestützt. Liegt eine wirksame Einwilligung der Betroffenen vor, ist die Durchführung eines DNA-Massenscreenings nach einem Beschluss des Bundesverfassungsgerichts (NJW 1996, S. 1587) grundsätzlich zulässig.

Das Staatsministerium der Justiz hat mir in Abstimmung mit dem Staatsministerium des Innern mitgeteilt, dass in Bayern keine generellen Vorgaben für die Durchführung solcher Massenscreenings existieren. Aus der Sicht des Staatsministerium der Justiz besteht für derartige Regelungen auch keine Notwendigkeit, weil ein Massenscreening in der Praxis aufgrund des damit verbundenen hohen Aufwands ohnehin nur in Betracht gezogen werde, wenn es sich um einen herausragenden Fall handele und die Straftat trotz erheblicher anderweitiger Anstrengungen nicht aufgeklärt werden konnte.

Aufgrund des mit der Durchführung eines DNA-Massenscreenings verbundenen sozialen Drucks auf den zur Teilnahme ausgewählten Personenkreis erscheint mir die auf die Einwilligung der Betroffenen gestützte Durchführung dieser Maßnahme nicht unproblematisch. Sie bedarf zumindest enger Grenzen und eines grundrechtssichernden Verfahrens. Die datenschutzrechtlichen Anforderungen an die Durch-

führung von DNA-Reihenuntersuchungen haben die Datenschutzbeauftragten des Bundes und der Länder in einem Positionspapier festgelegt, das ich dem Staatsministerium der Justiz und dem Staatsministerium des Innern zugeleitet habe. Darin wird die Beachtung folgender Kriterien gefordert:

- Anlasstat muss eine schwere, gegen die Rechtsgüter Leib oder Leben gerichtete Straftat sein.

- Gegenüber gesetzlich geregelten Ermittlungsmaßnahmen muss die DNA-Reihenuntersuchung subsidiär sein und als ultima ratio eingesetzt werden.

- Der Teilnehmerkreis muss durch eine Fallanalyse hinreichend eingegrenzt werden. Ein Massentest „ins Blaue hinein“ kann unter keinen Umständen zulässig sein.

- Die Tests müssen im Rahmen der Verhältnismäßigkeit in konzentrischen Kreisen durchgeführt werden, soweit der Kreis nicht klar und bestimmt ist. Eine Ausweitung auf den nächstgrößeren Kreis darf jeweils nur erfolgen, wenn die Maßnahme im engeren Kreis erfolglos geblieben ist.

- Die wirksame Einwilligung der Teilnehmer setzt sorgfältig gestaltete Formulare voraus, die insbesondere deutlich auf den Erhebungszweck, die Freiwilligkeit der Teilnahme und die Widerruflichkeit der Einwilligung sowie auf die Nutzung und Löschung der erhobenen Daten hinweisen. Diese Formulare müssen vorab übersandt werden, damit die Betroffenen ihre Entscheidung hinreichend und unbeeinflusst überdenken können. Die Maßnahmen zur Durchführung der DNA-Analyse (entsprechend § 81 f Abs. 2 StPO) einschließlich der zur Analyse in Frage kommenden Institute sind darzulegen. Missverständliche Hinweise auf die Möglichkeit der Erwirkung von Gerichtsbeschlüssen zur zwangsweisen Durchsetzung der Maßnahme dürfen in keinem Fall gegeben werden.

- Die erhobenen Daten müssen einer strengen Zweckbindung unterliegen. Sie dürfen nicht mit der DNA-Analyse-Datei des Bundeskriminalamts abgeglichen oder in diese eingestellt werden. Zweckdurchbrechende Nutzungen nach §§ 474 ff. StPO müssen ausgeschlossen sein.

- Nach einem Negativergebnis der Analyse sind die DNA-Probe und das DNA-Muster unverzüglich zu vernichten. Die gespeicherten Daten sind zu löschen, nach Abschluss des Verfahrens auch Namen und Negativergebnis.

- Die Verweigerung der Teilnahme allein darf keinen Anfangsverdacht begründen (BVerfG, NJW 96, S. 3071 ff.). Sie rechtfertigt es auch nicht, die Betroffenen als „andere Personen“ im Sinne von § 81 c StPO anzusehen.

- Die Verfahrensschritte sind hinreichend zu dokumentieren.

Ein DNA-Massenscreening habe ich bei dem durchführenden Polizeipräsidium geprüft. Anlass dieses Massenscreenings waren zwei Vergewaltigungen durch einen einzelnen Täter. Dabei war zuerst eine Reinigungskraft in einer Frauenklinik unter brutalen Umständen vergewaltigt worden. Am Tatort konnten DNA-Spuren des Täters gesichert werden. Einige Zeit später war dann in einer Schule eine Schülerin bis zur Bewusstlosigkeit gewürgt und vergewaltigt worden. Aufgrund der enormen Brutalität des Täters war die Polizei in diesem Fall auch von einem versuchten Tötungsdelikt ausgegangen. Die im zweiten Fall gesicherten DNA-Spuren hatten eine Übereinstimmung mit den Spuren in der Frauenklinik ergeben. Die in beiden Fällen durchgeführten Ermittlungen (Tatortarbeit, Zeugenvernehmungen, Lichtbildsuchungen, Öffentlichkeitsfahndung usw.) hatten zunächst zu keiner Täterfeststellung geführt. Aufgrund der herausragenden Bedeutung des Falles (besondere Tatumstände, starkes Medieninteresse, Sicherheitsgefühl der Bevölkerung, Hinweisaufkommen),vor allem aber wegen des Zeitdrucks aufgrund der besonderen Gefährlichkeit des Täters und der befürchteten Wiederholungsgefahr, wurde von der Polizei in Absprache mit der Staatsanwaltschaft eine DNA-Reihenuntersuchung durchgeführt.

Nach Angaben der Polizei hatte sich die Eingrenzung und Auswahl der von der Maßnahme Betroffenen für die ermittelnden Beamten schwierig gestaltet. Die Zeugen hatten den Täter sehr unterschiedlich beschrieben. Auch die Anzahl der Firmen, deren Mitarbeiter Zutritt zu Klinik und Schule gehabt hatten, war relativ groß gewesen. Durch die polizeiliche Öffentlichkeitsarbeit waren über 2.200 Hinweise eingegangen.

Die Betroffenen waren zum Teil durch „Einladungsschreiben“ zur Teilnahme aufgefordert worden. Problematisch erschien mir insbesondere die Formulierung im Einladungsschreiben:

„Sollten Sie an diesem freiwilligen Speicheltest nicht teilnehmen, besteht die Möglichkeit, einen entsprechenden Gerichtsbeschluss zu erwirken. Dies bedeutet, dass dann auch gegen Ihren Willen die Maßnahme durchgeführt werden kann und bei Ihnen unter

Umständen auch zwangsweise Blut abgenommen werden kann."

Mit dieser Formulierung wird der unzutreffende Eindruck erweckt, dass allein die Verweigerung der Einwilligung zwangsläufig zur gerichtlichen Anordnung der Maßnahme führe und der Betroffene lediglich eine Auswahl hinsichtlich des zur Maßnahme führenden Verfahrens habe. Das Bundesverfassungsgericht und verschiedene andere Gerichte haben aber entschieden, dass allein die Verweigerung der Blutentnahme nicht einen Anfangsverdacht gegen den Betroffenen begründen oder bestärken (und damit die zwangsweise Blutentnahme rechtfertigen) kann. Darauf habe ich das Staatsministerium der Justiz hingewiesen, das mir zugesagt hat, die Thematik zum Gegenstand einer Dienstbesprechung mit Vertretern von Staatsanwaltschaft und Polizei zu machen.

Auf meine Aufforderung hin hat mir die Polizei zugesagt, in künftigen Fällen die mit mir abgestimmten datenschutzrechtlichen Formulierungen des Musterschreibens des Staatsministeriums des Innern zu verwenden.

Unzureichend erschien mir auch, dass die Einwilligungsformulare und das dazugehörige Informationsblatt den Betroffenen erst unmittelbar vor der Probenentnahme ausgehändigt wurden. Den Betroffenen sollte aber ausreichend Zeit gegeben werden, das Informationsformular unbeeinflusst durchzulesen, den Inhalt aufzunehmen, sich ggf. beraten zu lassen und anschließend freiwillig zu entscheiden, ob sie an der Reihenuntersuchung teilnehmen wollen oder nicht. Die unmittelbare Aushändigung vor der Probenentnahme ist dafür grundsätzlich nicht ausreichend. Den Betroffenen sollten vielmehr regelmäßig mindestens 1 - 2 Tage Überlegungszeit eingeräumt werden.

Auf meinen Hinweis hin hat das Polizeipräsidium mir zugesagt, bei künftigen Reihenuntersuchungen die Einverständniserklärung und die dazugehörigen Hinweise bereits mit dem Einladungsschreiben an die Betroffenen zu versenden.

Zur Durchführung der Probenentnahme waren die Betroffenen zum Teil in ein Dienstgebäude der Polizei gebeten, zum Teil (Firmenangehörige und Zivildienstleistende) aber auch an ihren Arbeitsstätten aufgesucht worden. Dort waren Einwilligungserklärung und Hinweise ausgehändigt und unmittelbar anschließend - nach Erklärung der Einwilligung - die Probenentnahmen durchgeführt worden.

Abgesehen von der Kürze des den Betroffenen eingeräumten Überlegungszeitraums, ist das Aufsuchen der Arbeitsstelle und die damit verbundene Kenntnisnahme durch Kollegen und Vorgesetzten regelmäßig nicht verhältnismäßig und für die Freiwilligkeit der Einwilligung problematisch. Meiner Forderung, eine Probenentnahme nur in begründeten Ausnahmefällen an der Arbeitsstelle des Betroffenen durchzuführen, hat das Polizeipräsidium nicht widersprochen. Es hat dargelegt, dass derartige Ausnahmefälle z.B. bei Arbeitnehmern vorliegen können, die an wechselnden Einsatzorten tätig und deshalb schwer erreichbar sind. Auch im Hinblick auf die Gefahr weiterer Taten könne es zur Beschleunigung der Tataufklärung in Einzelfällen erforderlich sein, Probenentnahmen an der Arbeitsstelle der Betroffenen durchzuführen. Dies halte ich in besonderen Ausnahmefällen, wenn dem Betroffenen eine ausreichende Überlegungszeit unter angemessenen Umständen für eine freiwillige Einwilligung eingeräumt wird, grundsätzlich für vertretbar. Die abschließende Beurteilung der Wirksamkeit der Einwilligung muss der Kontrolle im Einzelfall vorbehalten bleiben.

Nachdem die Polizei zwischenzeitlich weitere DNA-Massenscreenings durchgeführt hat, beabsichtige ich, auch wegen Eingaben von Bürgern, zumindest ein weiteres Verfahren aus datenschutzrechtlicher Sicht zu prüfen. Mit der betreffenden Polizeidienststelle habe ich hierzu bereits Kontakt aufgenommen.

7.9 DNA-Analyse zur vorbeugenden Kriminalitätsbekämpfung bei vorläufig Festgenommenen

In meinem 20. Tätigkeitsbericht (Nr. 6.12.4) hatte ich über die problematische Verfahrensweise bei der Einholung von Einwilligungen für die DNA-Analyse bei vorläufig Festgenommen im Rahmen der Vernehmung berichtet. Ich habe dies zum Anlass genommen, auch im zurückliegenden Berichtszeitraum Prüfungen solcher Maßnahmen mit Schwerpunkt im Bereich der Betäubungsmittelkriminalität vorzunehmen.

Bei den geprüften Maßnahmen waren in der Regel überwiegend Personen betroffen, die im Rahmen der Schleierfahndung auf der Autobahn kontrolliert und bei denen erhebliche Mengen Rauschgift gefunden worden waren. Die Speichelproben seien in den meisten Fällen nach der Vernehmung im unmittelbaren Zusammenhang mit der Blutentnahme, Urinprobe und der erkennungsdienstlichen Behandlung entnommen worden. Zuvor seien dem Beschuldigten nach der Vernehmung die Einverständniserklärung und die Hinweise zur Einverständniserklärung ausgehändigt worden. Der Betroffene habe dann Gelegenheit gehabt, die ausgehändigten Unterlagen durchzulesen und sich zu entscheiden, ob er mit einer freiwilligen Speichelprobenentnahme und anschließender DNA-Analyse einverstanden sei. In etwa

98 Prozent der Fälle habe der Beschuldigte innerhalb von ca. 15 Minuten eingewilligt.

Die bei der Prüfung vorgelegten Einverständniserklärungen und Hinweise in deutscher Sprache stimmten inhaltlich mit den mit mir abgestimmten Formularen überein. In einem Fall waren betroffenen Albanern allerdings Formulare in albanischer Sprache vorgelegt worden, die einen ganz anderen Sachverhalt, nämlich die DNA-Analyse zum Vergleich mit Tatortspuren, betrafen. Nachdem die Maßnahme in diesem Fall auf der Grundlage von Einwilligungen durchgeführt wurde, die nicht auf einer umfassenden und zutreffenden Information über die vorgesehene Maßnahme beruhten (informierte Einwilligung), halte ich diese Einwilligungen nicht für wirksam. Ich habe die Polizeidienststelle deshalb aufgefordert, entweder richterliche Entscheidungen einzuholen oder die Speicherungen zu löschen, da der aktuelle Aufenthaltsort der Betroffenen der Polizei nicht bekannt ist.

Die betreffende Polizeidienststelle hat mir zugesagt, die vorliegenden fremdsprachigen Texte zu überprüfen und ggf. berichtigen zu lassen. Die DNA-Identifizierungsmuster wurden inzwischen vernichtet bzw. die Speicherungen in der DNA-Analyse-Datei gelöscht.

In erster Linie problematisch aber ist – abgesehen von meinen grundsätzlichen Vorbehalten gegen DNA-Analysen auf der Grundlage von Einwilligungen – die Frage der Wirksamkeit der unmittelbar nach einer polizeilichen Vernehmung eingeholten Einwilligungserklärungen. Die Speichelprobenentnahme und DNA-Analyse zum Zwecke der anschließenden Speicherung des DNA-Identifizierungsmusters beim Bundeskriminalamt stellt einen so erheblichen Eingriff in das Persönlichkeitsrecht des Betroffenen dar, dass die Durchführung dieser Maßnahme zu seinem Schutz vom Gesetzgeber unter den Vorbehalt einer richterlichen Entscheidung gestellt wurde. Eine Einwilligung des Betroffenen, die die richterliche Entscheidung ersetzen soll, kann allenfalls dann eine ausreichende Rechtsgrundlage für den Eingriff darstellen, wenn sie freiwillig und informiert erfolgt. Wenn der Betroffene im unmittelbaren Zusammenhang mit der Festnahme- und der Vernehmungssituation - und der damit in der Regel verbundenen psychischen Belastung - über die DNA-Maßnahme informiert und die Einwilligung von ihm abgegeben wird, ist das Vorliegen einer wirksamen Einwilligung zumindest zweifelhaft. Diese Zweifel werden bestärkt durch den unglaublich kurzen Zeitraum für Information, Überlegung und Entscheidung der meisten Betroffenen. Nachdem diese in den geprüften Fällen in der Regel ohnehin in Haft genommen wurden und deshalb eine Speichelprobenentnahme auch zu einem späteren Zeitpunkt möglich war, wäre die aus datenschutzrechtlicher Sicht erforderliche Einräumung einer ausreichenden Überlegungszeit (ca. zwei Tage) auch verfahrenstechnisch möglich gewesen. Ich habe deshalb die Polizei aufgefordert, den Betroffenen insbesondere in solchen Fällen eine ausreichende Überlegungszeit ohne engen zeitlichen Zusammenhang mir der Vernehmungssituation einzuräumen.

Die betreffende Polizeidienststelle möchte - nicht zuletzt wegen des damit verbundenen zusätzlichen Zeitaufwands für die Ermittlungsbeamten und im Hinblick auf eine arbeitsökonomische Verfahrensgestaltung - bei dem bisherigen Verfahren bleiben.

Inzwischen hat das Staatsministerium des Innern nach längerem Schriftwechsel folgende Verfahrensregelung getroffen:

- Belehrung und Aushändigung eines Informationsblattes erfolgen zeitlich in der Regel abgesetzt von den mit dem konkreten Strafverfahren zusammenhängenden Maßnahmen wie insbesondere einer Vernehmung.

- Dem Betroffenen wird vor Ort eine ausreichende Bedenkzeit eingeräumt. Eine konkrete Zeitvorgabe durch das Innenministerium ist insoweit nicht erfolgt.

- Nach Ablauf der Bedenkzeit ohne Entscheidung des Betroffenen ist grundsätzlich ein richterlicher Beschluss zu beantragen. Die Einholung einer Einwilligung des Betroffenen zu einem späteren Zeitpunkt soll nur ausnahmsweise erfolgen.

Die Anordnung des Innenministeriums stellt immerhin eine gewisse Verbesserung dar. Ich werde die praktische Umsetzung der Vorgaben beobachten.

7.10 Kontrolle einzelner Datenerhebungsmaßnahmen aufgrund Bürgereingaben

7.10.1 Erkennungsdienstliche Behandlung

Ein Bürger hatte sich an mich gewandt und um datenschutzrechtliche Prüfung seiner erkennungsdienstlichen Behandlung durch die Polizei gebeten. Zur polizeilichen Maßnahme war es auf Grund folgenden Vorfalls gekommen: Im Bereich der betroffenen Polizeiinspektion war in der Vergangenheit mehrfach eine Gruppe Jugendlicher aufgefallen, die im Verdacht stand, am Wochenende auf dem Weg von einer Diskothek zum S-Bahnhof Straftaten wie beispielsweise Sachbeschädigungen und Körperverletzungen begangen zu haben. In diesem Zusammenhang wurde eine Gruppe Jugendlicher von Zivilkräf-

ten der Polizei begleitet, um Straftaten, die von diesen ausgehen könnten, zu verhindern. Der Betroffene bestieg mit der Gruppe die S-Bahn und wurde dort später von Polizeibeamten kontrolliert. Dabei wurde festgestellt, dass der von ihm mitgeführte Fahrausweis für die Beförderungsstrecke nicht ausreichend war.

Der Betroffene, der bis dahin noch nicht polizeilich in Erscheinung getreten war, hatte sich mit seiner Kundenkarte und seinem Personalausweis ausweisen können. Er wurde trotzdem vorläufig festgenommen und zur Identitätsfeststellung und erkennungsdienstlichen Behandlung auf die Polizeiinspektion verbracht. Die Staatsanwaltschaft hat im Verfahren wegen des Verdachts des Erschleichens von Leistungen nach § 45 Abs. 1 Jugendgerichtsgesetz (JGG) von der Verfolgung abgesehen, da nach ihrer Ansicht die Schuld als gering anzusehen und der Betroffene strafrechtlich bisher noch nicht in Erscheinung getreten war.

Ich habe die erkennungsdienstliche Behandlung überprüft und als unzulässig beurteilt: Eine ED-Behandlung zum Zwecke der Durchführung des Strafverfahrens schied aus, da sich der Betroffene durch einen Personalausweis ausweisen konnte und sonstige Gründe für die Maßnahme im Rahmen des Strafverfahrens nicht ersichtlich waren. Eine erkennungsdienstliche Behandlung zum Zwecke des Erkennungsdienstes zu präventiv-polizeilichen Zwecken kam ebenfalls nicht in Betracht, da es sich bei dem Betroffenen zum einen nicht um einen gewerbs- oder gewohnheitsmäßigen Täter oder einen Rückfalltäter handelte. Auch im Hinblick auf Art und Schwere der Straftat war die ED-Behandlung nicht erforderlich. Das wäre insbesondere dann der Fall gewesen, wenn Anhaltspunkte dafür vorgelegen hätten, dass der Betroffene in ähnlicher oder anderer Weise erneut straffällig werden könnte und die erkennungsdienstlichen Unterlagen zur Förderung der dann zu führenden Ermittlungen geeignet erschienen wären. Der Betroffene war aber bisher noch nicht polizeilich in Erscheinung getreten. Von einer zukünftigen Begehung von solchen oder ähnlichen Straftaten auf Grund früherer Erkenntnisse konnte die Polizei deshalb zum Zeitpunkt der erkennungsdienstlichen Behandlung nicht ausgehen. Auch eine Zugehörigkeit des Betroffenen zu den von der Polizei verdächtigten Jugendlichen ließ sich nicht erkennen. Vielmehr ließen der vorliegende Sachverhalt wie auch die Feststellung der Staatsanwaltschaft auf eine geringe Schuld des Betroffenen schließen, so dass auch kein besonderes kriminalistisches Interesse an der Durchführung der erkennungsdienstlichen Behandlung bestand. Die erkennungsdienstliche Behandlung des 17-jährigen wegen des (einmaligen) Verdachts eines Vergehens des Erschleichens von Leistungen war deshalb unverhältnismäßig. Darüber hinaus bin ich von einem Fall geringerer Bedeutung ausgegangen, für den nach dem Polizeiaufgabengesetz kürzere Überprüfungsfristen festzusetzen sind. Die Polizei hat die erkennungsdienstlichen Unterlagen auf meine Aufforderung hin vernichtet und die betreffenden Daten gelöscht. Die Überprüfungsfrist für die Speicherung im KAN hat sie auf 3 Jahre verkürzt.

In einem weiteren Fall hatte sich ein Jugendlicher wegen einer seiner Ansicht nach unzulässigen erkennungsdienstlichen Behandlung an mich gewandt. Er war von einem anderen Jugendlichen, der eines Rauschgiftdelikts verdächtig war, gegenüber der Polizei beschuldigt worden, Marihuana mitgebracht und geraucht zu haben. Deswegen wurde der Petent einen Tag später ebenfalls als Beschuldigter vernommen. Für den vernehmenden Beamten nicht überraschend, gab er zwar an, an dem besagten Tag mit dem Mitbeschuldigten unterwegs gewesen zu sein, ein Konsum von Rauschgift habe jedoch nicht stattgefunden. Er habe nie mit Rauschgift zu tun gehabt und deswegen dem Mitbeschuldigten auch kein Rauschgift überlassen. Diese Angaben erschienen dem sachbearbeitenden Beamten auf Grund der durchgeführten Vernehmung glaubwürdig. Für ihn bestand der Eindruck, dass der Mitbeschuldigte den Petenten als Drogenlieferant belastet haben könnte, um von einer anderen Person abzulenken. Trotzdem wurden bei dem 15-jährigen Petenten erkennungsdienstliche Maßnahmen (Fotos, Fingerabdrücke) durchgeführt.

Auch in diesem Fall lagen die Voraussetzungen für eine erkennungsdienstliche Behandlung nicht vor. Weder war zum Zeitpunkt der Anordnung der ED-Behandlung das Vorhandensein möglicher weiterer Zeugen oder von Tatortspuren erkennbar, die einen Abgleich der gewonnenen Unterlagen gerechtfertigt hätten. Noch lag - auf Grund der Einschätzung des polizeilichen Sachbearbeiters - ein Tatverdacht von ausreichender Substanz vor, der die erkennungsdienstlichen Maßnahmen bei einem 15-jährigen Jungen zur vorbeugenden Kriminalitätsbekämpfung rechtmäßig hätten erscheinen lassen.

Nach Mitteilung des Innenministeriums wurde die Löschung bzw. Vernichtung der erkennungsdienstlichen Daten und Unterlagen veranlasst. Inzwischen seien auch alle im Zusammenhang mit diesem Vorgang erhobenen und im Kriminalaktennachweis gespeicherten Daten des Petenten gelöscht.

7.10.2 DNA-Analyse

Wegen einer Speichelprobenentnahme durch die Polizei zum Zwecke der DNA-Analyse hatte sich ein Bürger an mich gewandt und um datenschutzrechtliche Prüfung gebeten. Gegen ihn war von einer Frau

Anzeige wegen des Verdachts der gefährlichen Körperverletzung erstattet worden. Nach Angaben der Frau habe der Betroffene sie mit seinem Fahrzeug angefahren und anschließend geschlagen. Dieser räumte in seiner Beschuldigtenvernehmung nur eine verbale Auseinandersetzung ein. Weitere Zeugen konnten zu diesem Vorfall nicht ermittelt werden. Spuren, die der Tataufklärung hätten dienen können, wurden nicht gefunden. Offensichtliche körperliche Verletzungen an der Geschädigten konnten nicht festgestellt werden. Trotzdem wurde der Betroffene nach etwa drei Wochen erkennungsdienstlich behandelt und aufgrund seiner Einwilligung einer Speichelprobenentnahme zur DNA-Analyse zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren unterzogen. Die Staatsanwaltschaft stellte das Verfahren nach § 170 Abs. 2 StPO ein, da auf Grund der widersprüchlichen Aussagen der Beteiligten nicht festzustellen war, wie sich der Vorgang tatsächlich zugetragen hatte.

Die Voraussetzungen für die Durchführung einer DNA-Maßnahme gemäß § 81 g StPO lagen nicht vor. Zum einen hätte eine Straftat von erheblicher Bedeutung als Anlasstat vorliegen müssen. Zum anderen hätte eine ausreichend begründete Prognose die Annahme rechtfertigen müssen, dass gegen den Beschuldigten künftig weitere Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden.

Zwar ist der Tatbestand der gefährlichen Körperverletzung gemäß § 224 StGB als Regelbeispiel einer Straftat von erheblicher Bedeutung in § 81 g Abs. 1 StPO genannt. Nach der Rechtsprechung des Bundesverfassungsgerichts entbindet dies jedoch nicht von einer Einzelfallprüfung, ob der konkreten Straftat eine solche Bedeutung zukommt. Nach den Angaben der Anzeigeerstatterin ist ihr der Betroffene mit sehr geringer Geschwindigkeit an das Schienbein gefahren. Eine sichtbare Verletzung wurde dadurch nicht verursacht. Auch wenn ein solches Verhalten den Tatbestand des § 224 StGB erfüllen sollte, so liegt die Schwere der Tat im unteren Bereich, was für die Annahme einer erheblichen Bedeutung nicht ausreicht.

Es fehlt auch an der Begründung der Wiederholungsgefahr anhand schlüssiger, verwertbarer und nachvollziehbar dokumentierter Tatsachen. Allein die Angaben der Anzeigeerstatterin, dass sie der Betroffene im Rahmen einer verbalen Auseinandersetzung offensichtlich folgenlos mit seinem Fahrzeug berührt habe, genügt - ohne dass der Betroffene z.B. in vergleichbaren Situationen bereits früher strafrechtlich relevante Überreaktionen gezeigt hätte - für eine solche Maßnahme nicht.

Die Polizei hat die erkennungsdienstlichen Unterlagen und die Speichelprobe vernichtet sowie die im Kriminalaktennachweis und in der DNA-Analysedatei dazu gespeicherten personenbezogene Daten zur Person des Petenten gelöscht.

In einem anderen Fall hatte sich ein Bürger an mich gewandt, nachdem er von der Polizei zur Abgabe einer Speichelprobe zum Zwecke der DNA-Analyse aufgefordert worden war. Die Polizei war davon ausgegangen, dass der Betroffene wegen einer Straftat von erheblicher Bedeutung rechtskräftig verurteilt worden war und die entsprechende Eintragung im Bundeszentralregister noch bestand. Beides ist Voraussetzung für die polizeiliche Maßnahme. Eine entsprechende Auskunft (rechtskräftige Verurteilung des Betroffenen zu einem Jahr und sechs Monaten Jugendstrafe auf Bewährung wegen mehrfachen Diebstahls in besonders schweren Fällen) wollte die Polizei über das Bundeszentralregister eingeholt haben. Dies konnte aber auf Grund der Erkenntnisse meiner nachfolgenden Prüfung nicht sein. Die Polizei hatte keine Auskunft aus dem Bundeszentralregister eingeholt, sondern sich auf eine interne, nicht mehr aktuelle Datei verlassen.

Im Einzelnen:

Nach dem Bundeszentralregistergesetz (BZRG) beträgt die Tilgungsfrist im Bundeszentralregister für Jugendstrafen von nicht mehr als zwei Jahren, u.a. dann fünf Jahre, wenn die Vollstreckung zur Bewährung ausgesetzt ist. Nachdem bis zum Tag der Aufforderung zur Speichelprobe bereits mehr als 7 Jahre vergangen waren, hätte eine BZR-Auskunft zu diesem Zeitpunkt keinen Eintrag mehr ausweisen dürfen. Ich habe mich deshalb über den Bundesbeauftragten für den Datenschutz an das Bundeszentralregister gewandt. Von dort wurde mir mitgeteilt, dass keine Eintragungen über den Betroffenen mehr vorliegen. Zum gleichen Ergebnis kam auch die Staatsanwaltschaft, an die - nachdem der Bürger die Abgabe der Speichelprobe verweigert hatte - der Vorgang zur rechtlichen Prüfung und eventuellen Einholung eines richterlichen Beschlusses abgegeben worden war. Tatsächlich war die für die Durchführung der Maßnahme maßgebliche Auskunft nicht aus dem BZR, sondern aus der Datei „BZR-Auskunft Bayern - BABY“ eingeholt worden, eine Datei, die den Stand des Bundeszentralregisters zu einem ca. eineinhalb Jahre zurückliegenden Zeitpunkt wiedergab. Das LKA stellte die dort gespeicherten Daten einem beschränkten polizeilichen Nutzerkreis der Bayerischen Polizei im Online-Zugriff zur Verfügung, um kurzfristig zeitaufwändige Einholungen von BZR-Auskünften zu vermeiden. Auf eine Aktualisierung sei verzichtet worden, weil die Speicherungen bis 31.12.2003 befristet waren. Dies hätte den Anwendern der Datei nach Auskunft des Innenministeriums

und des LKA bekannt sein müssen, da diese auf den Charakter der Datei als reine Recherchedatei und die fehlenden Aussonderungsprüfungen und die damit verbundene Möglichkeit einer Inaktualität der Daten wiederholt hingewiesen worden seien. Deswegen sei in einer Dienstbesprechung des Staatsministeriums der Justiz und des Innern mit den Leitern der bayerischen Staatsanwaltschaften und den bayerischen Polizeipräsidenten festgelegt worden, dass auch eine nochmalige Anfrage beim Bundeszentralregister in den Fällen zu veranlassen ist, bei denen die Verurteilung des Betroffenen in erster Instanz zu einer Jugendstrafe, deren Vollstreckung zur Bewährung ausgesetzt wurde, mehr als 5 Jahre zurückliegt.

Im vorliegenden Fall hatte es die zuständige Polizeidienststelle unterlassen, vor der Aufforderung des Petenten zur Abgabe einer Speichelprobe einen aktuellen Auszug aus dem BZR einzuholen. Ausschließlich auf Grund der Weigerung des Betroffenen in die DNA-Analyse einzuwilligen, ist eine unzulässige Datenerhebung verhindert worden. Ich habe deshalb die Polizeidienststelle aufgefordert, zukünftig entsprechende Vorgaben umzusetzen bzw. seine nachgeordneten Dienststellen zur Umsetzung anzuhalten, um datenschutzrechtliche Verstöße zu vermeiden. Wegen der Möglichkeit, dass in den Jahren 2002 und 2003 weitere inaktuelle Bundeszentralregisterauskünfte als Grundlage für DNA-Analysen gedient hatten und es zu rechtswidrigen Speicherungen von DNA-Identifizierungsmustern in der DNA-Analyse-Datei gekommen war, war eine Überprüfung der retrograden DNA-Erfassungen dieser beiden Jahre erforderlich. Ich habe deshalb das Innenministerium gebeten zu prüfen, ob solche Maßnahmen auf der Grundlage inaktueller BZR-Auskünfte durchgeführt worden sind bzw. wie sichergestellt werden kann, dass keine unzulässigen Speicherungen in der DNA-Analyse-Datei eingetragen sind.

Nach einer Umfrage bei den betreffenden Polizeidienststellen geht das Innenministerium davon aus, dass es sich bei dem der Eingabe zugrundeliegenden Vorgang um einen Einzelfall handelt, der ausdrücklich bedauert wird. Eine weitergehende lückenlose Prüfung würde eine Sichtung und Bewertung aller 65.000 bayerischen Speicherungen in der DNA-Analysedatei notwendig machen. Im Hinblick darauf habe ich auf die Durchführung einer solchen Prüfung unter der Voraussetzung verzichtet, dass keine Hinweise auf einen weitergehenden fehlerhaften Umgang mit der Datei „BABY“ bekannt werden.

7.11 Datenschutzrechtliche Auswirkungen der Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff auf verdeckte polizeiliche Maßnahmen zur Gefahrenabwehr

Das Bundesverfassungsgericht hat in seinem Urteil vom 03.03.2004 grundlegende Ausführungen zu den verfassungsrechtlichen Anforderungen an die Wohnraumüberwachung zur Strafverfolgung sowie deren Grenzen gemacht. Auch wenn sich das Urteil direkt nur auf die repressive Wohnraumüberwachung bezieht, sind die dort aufgestellten Grundsätze auch für verdeckte polizeiliche Maßnahmen zur Gefahrenabwehr, die in Grundrechte der Betroffenen eingreifen, von Bedeutung. Dies gilt insbesondere für die Regelungen zur präventiven Wohnraumüberwachung in Art. 34 PAG. Ausgangspunkt der Entscheidung ist der intensive Eingriff in das Grundrecht der Unverletzlichkeit der Wohnung nach Art. 13 Grundgesetz (GG) und der Schutz des Kernbereichs privater Lebensgestaltung. Die Grundsätze des Bundesverfassungsgerichts sind aufgrund der gleichen Ausgangslage und Schutzwürdigkeit der Betroffenen auch auf Wohnraumüberwachungsmaßnahmen nach dem Polizeiaufgabengesetz zu übertragen.

Darüber hinaus hat das Bundesverfassungsgericht in seinem Beschluss vom 03.03.2004 dem Gesetzgeber aufgegeben, bei einer Neuregelung der Überwachungsbefugnisse zur Straftatenverhütung im Außenwirtschaftsgesetz auch die Grundsätze zu beachten, die das Gericht unter anderem in seinem Urteil zur akustischen Wohnraumüberwachung niedergelegt hat. Vor diesem Hintergrund und im Hinblick auf die Heimlichkeit der Überwachung und ihrer möglichen Berührung mit dem Kernbereich privater Lebensgestaltung halten die Datenschutzbeauftragten des Bundes und der Länder es für geboten, alle Formen verdeckter Datenerhebung zu präventiven Zwecken an den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 03.03.2004 auszurichten und die einschlägigen gesetzlichen Befugnisregelungen zu überprüfen und ggf. neu zu fassen.

Neben der Befugnis zur Wohnraumüberwachung gibt es eine Reihe von weiteren verdeckten polizeilichen Datenerhebungsmaßnahmen, die in den absolut geschützten Kernbereich privater Lebensgestaltung eingreifen können, wie z.B. der Einsatz technischer Mittel zum Abhören des nicht öffentlich gesprochenen Wortes (außerhalb von Wohnungen) oder die längerfristige Observation. Zur Entfaltung der Persönlichkeit in diesem Kernbereich gehört die Möglichkeit, Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, ohne Angst, dass staatliche Stellen dies überwachen. Dieser aus der Menschenwürdegarantie des Art. 1 Abs. 1 GG abzu-

leitender unantastbare Kernbereich ist nach den Ausführungen des Bundesverfassungsgerichts bei jeder staatlichen Beobachtung zu wahren.

7.12 Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes

Am 22.04.2003 wurde von der CSU-Fraktion ein Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes beim Bayerischen Landtag eingebracht. Gegen diesen Entwurf - der eine Änderung der Regelungen der Wohnraumüberwachung noch nicht enthielt - hatte ich insbesondere im Hinblick auf die Regelung der präventiven Telekommunikationsüberwachung wegen eines zu weiten und offenen Straftatenkatalogs und wegen des fehlenden Schutzes von sog. Berufsgeheimnisträgern vor Überwachung grundlegende Bedenken erhoben. Am 01.07.2003 fand im Landtag eine Sachverständigenanhörung zum Thema „präventive Telekommunikationsüberwachung“ statt, bei der sich unter anderem Vertreter von Wissenschaft, Berufsgeheimnisträgern, Staatsanwaltschaft und Polizei zu den geplanten Änderungen geäußert haben. Auch aufgrund der von meiner Seite geäußerten Kritik wurde der Gesetzentwurf schließlich zurückgezogen.

Am 02.07.2004 habe ich vom Staatsministerium des Innern auf Nachfrage einen Referentenentwurf zur Änderung des Polizeiaufgabengesetzes erhalten.

Der Gesetzentwurf enthält weitreichende Ergänzungen der polizeilichen Befugnisse, insbesondere für die automatisierte Kennzeichenerkennung und die präventive Telekommunikationsüberwachung. Beide Maßnahmen gibt es bisher in Bayern nicht. Außerdem sollen die Vorschriften zur präventiven Wohnraumüberwachung an die Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff angepasst werden.

Hier ist im Übrigen anzumerken, dass in einem weiteren Schritt auch andere verdeckte Datenerhebungsmaßnahmen anhand der Maßstäbe des Urteils des Bundesverfassungsgerichts auf den Prüfstand müssen.

Zu dem Gesetzentwurf habe ich gegenüber dem Staatsministerium des Innern ausführlich Stellung genommen. In einer weiteren Besprechung hatte ich Gelegenheit, nochmals auf die wichtigsten datenschutzrechtlichen Gesichtspunkte hinzuweisen. Wesentliche Teile meiner Anregungen sind in weiteren Änderungen, zuletzt vom 05.11.2004, eingeflossen.

Eine Zusammenfassung der wichtigsten datenschutzrechtlichen Gesichtspunkte enthalten die folgenden Darstellungen.

7.12.1 Straftatenkatalog

Voraussetzung für die Durchführung der präventiven Wohnraumüberwachung und Telekommunikationsüberwachung soll nach dem Entwurf unter anderem das Vorliegen von Tatsachen sein, die die begründete Annahme rechtfertigen, dass bestimmte Personen eine „schwerwiegende Straftat“ begehen werden. Diese Straftaten sind nunmehr in einem abschließenden Katalog von 10 Straftatengruppen aufgeführt.

Das Bundesverfassungsgericht hat in seinem Urteil vom 03.03.2004 zum Großen Lauschangriff zur Strafverfolgung entschieden, dass nur das Vorliegen von Straftaten von besonderer Schwere den Eingriff in die Privatsphäre der Wohnung rechtfertigen könne. Dabei sei von der besonderen Schwere einer Straftat nur dann auszugehen, wenn sie der Gesetzgeber mit einer höheren Höchststrafe als 5 Jahre Freiheitsstrafe bewehrt hat.

Diese Grundsätze müssen auch für die präventive Wohnraum- und Telekommunikationsüberwachung gelten (vgl. oben Nr. 7.11). Aufgrund der mit mir geführten Gespräche entspricht die ganz überwiegende Mehrzahl der in dem Katalog nunmehr enthaltenen Straftatbestände diesen Vorgaben.

Allerdings sind in dem Katalog entgegen den Vorgaben des Bundesverfassungsgerichts in dem Urteil zur technischen Wohnraumüberwachung noch einige wenige Tatbestände enthalten, die mit einer Freiheitsstrafe unter oder bis zu fünf Jahren bedroht sind. Ich habe gegenüber dem Staatsministerium des Innern gefordert, auch diese Tatbestände aus dem Katalog herauszunehmen oder wenigstens den Zusatz aufzunehmen, dass die Tat im Einzelfall besonders schwer wiegen muss. Das ist bis Redaktionsschluss dieses Berichts nicht geschehen.

7.12.2 Präventive Wohnraumüberwachung

Bereits nach dem geltenden Polizeiaufgabengesetz ist die präventive Wohnraumüberwachung unter bestimmten Voraussetzungen zulässig (Art. 34 PAG). Sie erlaubt der Polizei nicht nur die akustische sondern auch die optische Überwachung auch der zu Wohnzwecken genutzten Räume. Aufgrund der Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff besteht ein erheblicher Änderungsbedarf, da die gesetzlichen Bestimmungen an die vom Bundesverfassungsgericht zum Schutz des Kernbereichs der privaten Lebensgestaltung aufgestellten Grundsätze anzupassen sind. Mit der Neufassung von Art. 34 PAG unternimmt das Staatsministerium des Innern diese Anpassung, wobei es zahlrei-

che Forderungen und Anregungen meinerseits aufgenommen hat:

- Da Anknüpfungspunkt für die Maßnahme nicht der Verdacht einer bereits begangenen Straftat sondern die Annahme eines zukünftigen Verhaltens des Betroffenen ist, muss deutlich zum Ausdruck kommen, dass die objektiv begründete Annahme der Begehung einer schwerwiegenden Straftat, also zumindest eine konkrete Gefahr ihrer Verwirklichung, vorliegen muss. Es muss klar erkennbar sein, dass nicht nur auf subjektive Komponenten abgestellt wird, die sich möglicherweise im Nachhinein für die Gefahr der Verwirklichung einer schwerwiegenden Straftat als irrelevant erweisen. Dies wird nunmehr dadurch verdeutlicht, dass die Maßnahme erst dann zulässig sein soll, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass diese Personen eine schwerwiegende Straftat begehen **werden (nicht „wollen").** Ich hätte darüber hinaus eine ergänzende Erläuterung in der Gesetzesbegründung begrüßt, wonach eine Sachlage vorliegen muss, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall mit hinreichender Wahrscheinlichkeit zur Begehung einer schwerwiegenden Straftat führt (konkrete Gefahr).

- Das Bundesverfassungsgericht zählt das Seelsorgehilfegespräch mit einem Geistlichen und das Gespräch mit einem Strafverteidiger zum Kernbereich privater Lebensgestaltung, denen zur Wahrung der Menschenwürde eine wichtige Funktion zukommt. Solche Gespräche können auch einen Bezug zu den genannten Straftaten haben. Gleichwohl müssen sie geschützt bleiben. Der Entwurf sieht demgemäß nunmehr vor, dass eine Wohnraumüberwachung auch dann unterbleibt, wenn das Gespräch mit den obigen Berufsgeheimnisträgern einen unmittelbaren Bezug zu den genannten Gefahren oder Straftaten aufweist. Eine Ausnahme kann dann zulässig sein, wenn ein Angehöriger dieser Berufsgruppen unmittelbar in die geplante Tat involviert ist oder die Gefahr vom Berufsgeheimnisträger selbst ausgeht.

- Bei Gefahr im Verzug sieht der Gesetzentwurf nunmehr vor, dass die Maßnahme durch den Dienststellenleiter angeordnet werden kann und eine „Bestätigung durch den Richter unverzüglich einzuholen ist". Mit dieser Änderung der ursprünglichen Formulierung „eine richterliche Entscheidung ist unverzüglich nachzuholen" gehe ich davon aus, dass die richterliche Entscheidung auf die ursprüngliche Anordnung des Dienststellenleiters zurückwirkt. Dies halte ich für unbedingt erforderlich, da es bei Eingriffen dieser Tiefe keine gerichtsfreien Räume geben darf.

Nicht aufgenommen wurde dagegen die nachstehende Forderung:

- Die engsten Familienangehörigen und Vertrauten, bei denen eine Überwachung von Gesprächen grundsätzlich nicht zulässig ist, sind nicht deckungsgleich mit den aus persönlichen Gründen Zeugnisverweigerungsberechtigten nach § 52 StPO. Aber auch soweit letztere keine besonderen Vertrauenspersonen sind, haben sie ein Zeugnisverweigerungsrecht.

  Dieses Recht würde ausgehöhlt, wenn bezüglich ihrer Person keine Verwendungsbeschränkungen bestehen würden. Ich habe dem Staatsministerium des Innern mitgeteilt, dass vorgesehen werden sollte, dass in den Fällen des § 52 StPO aus einer präventiven Wohnraumüberwachung gewonnene Erkenntnisse nur verwertet werden dürfen, wenn dies unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts steht.

Sehr problematisch ist auch die grundsätzliche Möglichkeit einer nur automatischen Datenerhebung aus Wohnungen; wegen der Unterbrechungspflicht bei Kernbereichsgesprächen „kann (es notwendig sein), „bei dem Abhören einer Privatwohnung auf eine nur automatische Aufzeichnung der abgehörten Gespräche zu verzichten, um jederzeit die Ermittlungsmaßnahme unterbrechen zu können" so BVerfG aaO Rdnr. 151 a.E. Immerhin hat das Innenministerium auf unseren Hinweis das vorherige Regel-Ausnahmeverhältnis zu Gunsten einer Einschränkung einer nur automatischen Aufzeichnung umgedreht. Jedenfalls sollte die Methode der Aufzeichnung in der Begründung nach Art. 34 Abs. 4 Satz 3 E angegeben werden, damit der Richter die Zulässigkeitsvoraussetzungen einer nur automatischen Aufzeichnung überprüfen kann.

7.12.3 Präventive Telekommunikationsüberwachung

Die vorgesehene Regelung der präventiven Telekommunikationsüberwachung (TKÜ) setzt eine Entwicklung in der Gesetzgebung fort, der Polizei immer wieder neue, zum Teil tiefgreifende Eingriffsbefugnisse einzuräumen, die das Recht auf informationelle Selbstbestimmung berühren. Das ist auch deswegen von erheblicher Relevanz, weil von solchen Maß-

nahmen nicht nur Verantwortliche oder Störer im Sinne des Polizeirechts betroffen sind, sondern in großem Umfang auch und gerade Nichtverantwortliche und Nichtstörer. Im Hinblick auf die Aufgabe der Polizei, Straftaten zu verhindern, sehe ich gleichwohl unter bestimmten engen Voraussetzungen diese Maßnahme für vertretbar an. Durch eine klare Formulierung der Eingriffsvoraussetzungen muss aber vermieden werden, dass - im Gegensatz zur Wohnraumüberwachung - sich die präventive Telekommunikationsüberwachung an die negative Entwicklung der repressiven Telekommunikationsüberwachung anschließt. Zahlen zur Telekommunikationsüberwachung nach § 100 a StPO zeigen für die letzten Jahre eine besorgniserregende Entwicklung. Die Erhöhung der Gesamtzahl der Überwachungsmaßnahmen von 1990 bis 2000 von ca. 2.500 auf ca. 15.750 wird zu einem Teil mit dem sog. Handy-Boom zu erklären sein. Ich habe aber erhebliche Zweifel, ob dies auch für die stetig weitere Erhöhung in den folgenden Jahren gilt (z.B. 2002: 21.874; 2003: 24.441). Der Umfang der Eingriffe in Kommunikationsinhalte wird noch deutlicher durch die Zahl der in ihrem Recht auf vertrauliche Kommunikation Betroffenen. Nach dem Gutachten des Max-Planck-Instituts Freiburg sind bei 21 %, also ca. einem Fünftel der Anordnungen, jeweils 1.000 bis 5.000, in weiteren 8 % jeweils über 5.000 Gespräche abgehört worden.

Noch viel häufiger wird schließlich von der Möglichkeit Gebrauch gemacht, Verbindungsdaten abzufragen: So sollen 2001 1,5 Mio., 2002 2,0 Mio. und 2003 2,7 Mio. Anfragen von Sicherheitsbehörden bei Telekommunikationsanbietern vorgelegen haben. Hinzu kommt die sog. Zielwahlsuche, bei der ermittelt wird, von welchen Anschlüssen aus Telefonate mit dem überwachten Anschluss geführt worden sind und in die jede der ca. 216 Mio. täglich hergestellten Telefonverbindungen einbezogen wird.

Die Gefahr des Ausuferns von TKÜ-Maßnahmen auch im präventiven Bereich besteht auch deswegen, weil nur automatisierte Aufzeichnungen im Gegensatz zu den Wohnraumüberwachungsmaßnahmen mit technischen Mitteln („großer Lauschangriff“) nicht auf Ausnahmefälle beschränkt bleiben sollen.

In einer ausführlichen Stellungnahme hatte ich das Staatsministerium des Innern auf eine Vielzahl, zum Teil grundlegender Forderungen hingewiesen, die eine Änderung der Vorschriften erforderlich machten. Insbesondere ist es notwendig, dass die präventive Telekommunikationsüberwachung auf der Grundlage hinreichend bestimmter und angemessener Tatbestandsvoraussetzungen erfolgt und dass die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit gewahrt werden.

Bei der präventiven Telekommunikationsüberwachung sind die Eingriffsvoraussetzungen im Vergleich zur repressiven Telekommunikationsüberwachung naturgemäß erheblich unbestimmter - es fehlt die objektive Tatsache einer begangenen Straftat -, so dass hier neben der Gefahr einer zahlenmäßigen Ausweitung die Gefahr einer Ausweitung der Maßnahme hin zu einem Verdachtsschöpfungsinstrument besteht. Auf meine Forderung hin wurde der Gesetzentwurf deswegen dahingehend geändert, dass Anknüpfungspunkt für die Maßnahme nicht mehr ist, dass Personen ein im Einzelnen bezeichnetes Verhalten zeigen „wollen“. Diese Formulierung wurde durch „werden“ ersetzt. Zusätzlich würde ich eine Klarstellung in der Begründung begrüßen, dass insoweit die objektive Gefahr der Begehung einer bestimmten schwerwiegenden Straftat (vgl. Nr. 7.12.1), also eine konkrete Gefahr ihrer Verwirklichung vorliegen muss.

Daneben haben eine ganze Reihe meiner Forderungen und Anregungen Aufnahme in den Gesetzentwurf gefunden. Als Schwerpunkte seien angeführt:

- Der Straftatenkatalog wurde auf bestimmte schwerwiegende Straftaten beschränkt (vgl. Nr. 7.12.1)

- Die Eingriffsvoraussetzungen zur Abwehr von Gefahren für Personen wurden auf die Abwehr von Gefahren für Leib oder Leben beschränkt (anstatt auch Abwehr von Gesundheitsgefahren)

- Wie bei der Wohnraumüberwachung wurde auch bei der TKÜ klargestellt, dass der Schutz für alle Berufsgruppen und Berufshelfer nach §§ 53,53 a StPO gilt.

- Im Fall einer Kernbereichsverletzung und einem darauf beruhenden Verwertungsverbot der gewonnenen Daten werden diese unverzüglich gelöscht. Der Schutz erstreckt sich damit nicht nur auf Berufsgeheimnisträger, sondern auch auf besonders Vertraute im Sinn der Rechtsprechung des Bundesverfassungsgerichts. Allerdings fehlt im Gegensatz zu der Regelung betreffend die Berufsgeheimnisträger insoweit ein ausdrückliches Verbot der Datenerhebung (dazu siehe unten)

- Meine Forderung nach Dokumentation der Löschung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, wurde im Gesetzestext aufgenommen.

Nicht aufgenommen wurde u.a. im Gegensatz zu meinen Forderungen:

- Eine Berichtspflicht an den Landtag und eine Evaluierungspflicht. Für die Wohnraumüberwachung besteht eine solche Berichtspflicht nach Art. 34 Abs. 6 Entwurf. Eine Berichts- und Evaluierungspflicht halte ich vor allem im Hinblick auf die oben dargestellten Gefahren der Ausweitung der präventiven TKÜ zu Kontrollzwecken unbedingt für erforderlich.

- Ein Datenerhebungsverbot für Gespräche, die dem „Kernbereich privater Lebensgestaltung“ zuzurechnen sind; die hierzu aufgenommene Löschungspflicht stellt immerhin eine Verbesserung dar. Es sind aber für mich keine Gründe ersichtlich, warum nicht auch für diesen Kreis entsprechend der Regelung der Berufsgeheimnisträger ein Erhebungsverbot statuiert wird, wenn bei der Durchführung der Maßnahme erkennbar wird, dass solche Gespräche geführt werden.

- Eine Regelung für zeugnisverweigerungsberechtigte Personen nach § 52 StPO; nicht alle der dort aufgeführten sind dem „Kernbereich privater Lebensgestaltung“ im Sinn des Art. 34 c Abs. 6 Entwurf zuzurechnen; ich hatte vorgeschlagen eine Verwertung dieser Erkenntnisse nur zuzulassen, wenn dies unter Berücksichtigung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis steht.

Insgesamt kann ich aber feststellen, dass der nun vorliegende Entwurf wesentliche Bedenken von mir ausgeräumt hat.

7.12.4 Automatisierte Kennzeichenerkennung

Nach Erprobung der automatisierten Kennzeichenerkennung im Rahmen eines von mir akzeptierten Pilotprojekts auf einer Autobahn und an zwei Grenzübergängen soll diese Maßnahme in das Polizeiaufgabengesetz aufgenommen werden, nachdem ich einem Dauerbetrieb ohne bereichsspezifische gesetzliche Regelung nicht zugestimmt hatte. Sie soll nicht flächendeckend durchgeführt, sondern auf bestimmte Bereiche beschränkt werden, in denen jetzt schon eine Identitätsfeststellung zulässig ist. Wenn ich auch den vorgesehenen Einsatz von automatisierten Kennzeichenerkennungssystemen im Straßenverkehr nicht ohne Sorge betrachte, weil diese Maßnahme einen Schritt zum Aufbau einer Überwachungsinfrastruktur darstellt, so halte ich den mit der Datenerhebung und dem Abgleich verbundenen Eingriff doch für hinnehmbar, wenn er in engen Grenzen, mit der geringstmöglichen Belastung vorgenommen wird, insbesondere wenn er sich auf den Abgleich mit Fahndungsdateien beschränkt und Nichttrefferfälle spurlos gelöscht werden.

Auf meine diesbezüglichen Forderungen hin wurde der Abgleich grundsätzlich auf den Fahndungsbestand beschränkt, der Abgleich mit anderen polizeilichen Dateien nur insoweit zugelassen, als die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehenden Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist. Damit sehe ich die Verhältnismäßigkeit dieser Maßnahme als gewahrt an. Der Abgleich mit z.B. Vorgangsverwaltungsdateien ist damit ausgeschlossen.

Weiter ist nunmehr auch durch den Gesetzestext klargestellt, dass die durch den Einsatz automatisierter Kennzeichenerkennungssysteme erlangten personenbezogenen Daten unverzüglich zu löschen sind, wenn der Datenabgleich keinen Treffer ergibt.

7.13 Videoüberwachung öffentlicher Straßen und Plätze

7.13.1 Videoüberwachung in Innenstadtbereichen

In meinem letzten Tätigkeitsbericht (Nr. 6.13) hatte ich über die Einführung einer gesetzlichen Regelung der polizeilichen Videoüberwachung öffentlicher Straßen und Plätze berichtet. Zur Erläuterung dieser Regelung hat das Staatsministerium des Innern zwischenzeitlich die Bekanntmachung zum Vollzug des Polizeiaufgabengesetzes geändert. Meine Bedenken und Anregungen bezüglich der Vollzugsbekanntmachung wurden vom Staatsministerium des Innern leider größtenteils nicht berücksichtigt. So hatte ich vorgeschlagen, angesichts der besonderen Sensibilität der Videoaufnahmen den Zugriff auf einen begrenzten Personenkreis zu beschränken und die Notwendigkeit einer entsprechenden innerdienstlichen Festlegung in die Vollzugsbekanntmachung aufzunehmen. Dem ist das Staatsministerium des Innern jedoch mit dem Argument entgegengetreten, es sei ausreichend, wenn sich der Zugriff nach den bereits vorhandenen organisatorischen Zugriffsbeschränkungen der jeweiligen Dienststelle richte. Meine weitere Forderung nach einer nachvollziehbaren Protokollierung der Zugriffe auf die Videobänder wurde ohne jegliche Begründung nicht übernommen. Einen ausdrücklichen Hinweis darauf, dass es sich bei der gesetzlichen Speicherungsfrist um eine Höchstfrist handelt, hielt das Staatsministerium des Innern ebenfalls für entbehrlich.

Meine Kritik bezieht sich im wesentlichen jedoch auf die Erläuterung der Orte, an denen eine Videoüberwachung vorgenommen werden darf. Ich hatte diesbezüglich gefordert, in der Vollzugsbekanntmachung darauf hinzuweisen, dass eine Videoüberwachung zu Zwecken der Kriminalitätsbekämpfung nur an solchen Orten zulässig ist, die eine besondere Kriminalitätsbelastung aufweisen, die sich also deutlich von der an anderen Orten abhebt. Durch diese Einschränkung wird zum einen der Schwere des mit der Maßnahme verbundenen Grundrechtseingriffs Rechnung getragen, zum anderen wirkt sie einer zu weitgehenden Ausdehnung der Videoüberwachung in zentralen Innenstadtgebieten entgegen. Darüber hinaus sollte darauf hingewiesen werden, dass zur Begründung der Erforderlichkeit einer Videoüberwachung an bestimmten Örtlichkeiten zuvor eine auf einen bestimmten Zeitraum und diese Örtlichkeiten bezogene Aufstellung der begangenen Straftaten zu erstellen ist. Diese Feststellungen sollen der Prüfung, ob die für die Videoüberwachung vorgesehenen Örtlichkeiten als Kriminalitätsschwerpunkt angesehen werden können, zugrunde gelegt werden. Schließlich sollte in regelmäßigen Abständen eine Evaluierung durchgeführt werden, um zu überprüfen, ob die Voraussetzungen für eine Videoüberwachung noch vorliegen.

Auch diese Forderungen hat das Staatsministerium des Innern mit der Begründung abgelehnt, Art. 32 Abs. 2 PAG verlange nicht, dass an den genannten Örtlichkeiten bereits Straftaten oder Ordnungswidrigkeiten begangen worden sind. Die Vorschrift verlange nur tatsächliche Anhaltspunkte dafür, dass an einem Ort die gesetzlichen Voraussetzungen erfüllt sind. Tatsächliche Anhaltspunkte könnten sich aus der allgemeinen Erfahrung ergeben, wonach bestimmte Orte besonders kriminalitätsanfällig sind.

Dieser Ansicht bin ich entgegengetreten. Die gesetzliche Regelung stellt auf eine Prognoseentscheidung für die Zukunft ab. Um diese Prognosenentscheidung treffen zu können, ist es erforderlich, die Vorkommnisse an dem zu beurteilenden Ort in der Vergangenheit zu betrachten. Die allgemeine Erfahrung, dass bestimmte Orte besonders kriminalitätsanfällig sind, kann jedenfalls nicht ausreichen. Die Prognoseentscheidung muss vielmehr aufgrund tatsächlicher Erkenntnisse für den konkreten Fall getroffen werden. Andernfalls bestünde die Gefahr, dass gerade in einer Großstadt, in der erfahrungsgemäß im Innenstadtbereich allgemein mehr Straftaten begangen werden, mit eben dieser Argumentation fast an jedem beliebigen Ort Videokameras aufgestellt werden könnten. Eine solche Auslegung, bei der die Gefahr einer flächendeckenden Videoüberwachung besteht, ist abzulehnen.

Der Verwaltungsgerichtshof Baden-Württemberg hat dazu in seinem Urteil vom 21.07.2003 ausgeführt, dass ein Kriminalitätsschwerpunkt, der die Videoüberwachung rechtfertigt, eine besondere Kriminalitätsbelastung aufweisen müsse, die sich deutlich von der an anderen Vergleichsorten innerhalb derselben Stadt abhebt. Zur wirksamen Kontrolle der Lagebeurteilung sei die nachvollziehbare Dokumentation anhand aktueller spezifischer örtlicher Lagebilder, unter besonderer Berücksichtigung der Straßenkriminalität und anderer Straftaten, die das Sicherheitsgefühl der Bevölkerung besonders beeinträchtigen, erforderlich. Dabei wird ausdrücklich hervorgehoben, dass eine allgemeine Statistik über die Kriminalitätsbelastung (z.B. im ganzen Innenstadtquadranten) nicht ausreichend ist, sondern sich konkret auf die zu überwachende Örtlichkeit im Vergleich zur Straßenkriminalität im gesamten Stadtgebiet, der Innenstadt oder vergleichbaren Örtlichkeiten beziehen muss.

Trotz der von mir geäußerten Bedenken hat das Staatsministerium des Innern die Änderung der Vollzugsbekanntmachung zum Polizeiaufgabengesetz bekannt gemacht. Ich werde deshalb jede geplante polizeiliche Videoüberwachung unabhängig von diesen Verwaltungsvorschriften daraufhin überprüfen, ob die gesetzlichen Voraussetzungen erfüllt sind. Eine rechtzeitige Beteiligung an solchen Planungen habe ich erbeten.

Die im Berichtszeitraum von der Münchner Polizei neu eingerichtete Videoüberwachung am Münchner Bahnhofsvorplatz und am Stachusrondell habe ich entsprechend geprüft. Zu diesem Zweck habe ich mir eine Kriminalitätsstatistik vorlegen lassen, in der nicht nur die registrierten Straftaten im Bereich der zu überwachenden Plätze, sondern auch andere, vergleichbare Örtlichkeiten enthalten waren. Anhand der detaillierten Aufstellungen der jeweils dort erfassten Straftaten habe ich feststellen können, dass am Münchner Hauptbahnhof und Stachusrondell deutlich mehr Straftaten, die der Straßenkriminalität zuzurechnen sind, in den Zeiträumen 2001 bis 2003 angezeigt wurden, als an vergleichbaren Örtlichkeiten im Innenstadtbereich. Darüber hinaus war insbesondere am Bahnhofsvorplatz eine deutliche Zunahme der Delikte im Jahre 2003 gegenüber den Vorjahreszeiträumen zu beobachten. Im Hinblick auf die der Videoüberwachung zugrundeliegende Kriminalitätsstatistik habe ich keine Bedenken gegen die Videoüberwachung geäußert.

Was die Aufstellung der Schilder betrifft, die auf die Videoüberwachung hinweisen, hat eine Ortsbesichtigung ergeben, dass an wichtigen Zugangswegen für Passanten Schilder fehlen. Im Übrigen sind die Hinweisschilder farblich unauffällig gestaltet. Dazu kommt, dass sie in relativ großer Höhe angebracht sind. Ich habe das Polizeipräsidium München darauf hingewiesen und habe bezüglich der Aufstellung der Schilder im Rahmen einer gemeinsamen Ortsbesich-

tigung eine ausreichende Ergänzung gefordert. Da mir die Polizei zwischenzeitlich mitgeteilt hat, dass die Ergänzung an der ablehnenden Haltung der Stadt München zu scheitern drohe, habe ich mich an den Oberbürgermeister sowie den Leiter der Stadtwerke mit der Bitte um Unterstützung gewandt.

Soweit auf den überwachten Plätzen Versammlungen stattfinden, sind Videoaufzeichnungen von Versammlungsteilnehmern nur unter den engen Voraussetzungen der §§ 12 a, 19 a Versammlungsgesetz zulässig. Ich habe das Polizeipräsidium München um Mitteilung gebeten, wie in diesen Fällen mit der Videoüberwachung verfahren wird. Dieses hat mir daraufhin mitgeteilt, dass die Kameras eingeschaltet bleiben, auch wenn an den überwachten Bereichen Versammlungen stattfinden. Es würden jedoch grundsätzlich nur Übersichtsaufnahmen gefertigt. Die Anfertigung von Einzelaufnahmen (Zoomen) sei technisch allerdings auch bei Versammlungen jederzeit möglich. Unter den gesetzlichen Voraussetzungen würden daher auch personenbezogene Bilder aufgenommen werden. Das Zoomen werde nicht protokolliert.

Ein solches Verfahren halte ich nicht für ausreichend, um die Einhaltung der gesetzlichen Vorschriften zum Schutz des Grundrechts auf Versammlungsfreiheit zu gewährleisten. Diesem Grundrecht gebührt nach der Rechtsprechung des Bundesverfassungsgerichts ein besonderer Rang, da es als Zeichen der Freiheit, Unabhängigkeit und Mündigkeit des selbstbewussten Bürgers in einem freiheitlichen Staatswesen anzusehen ist. Art. 8 Abs. 1 Grundgesetz garantiert das möglichst unbeeinflusste Engagement des Einzelnen vor und bei Versammlungen und schützt damit auch davor, das Grundrecht im Visier von Polizei oder Verfassungsschutz wahrnehmen zu müssen. Schon die Kenntnis, dass die Videokameras am Hauptbahnhof und Stachus während der Versammlungen eingeschaltet bleiben, könnte Auswirkungen auf die Unbefangenheit der Versammlungsteilnehmer haben und damit ihre grundrechtlich geschützten Rechte beeinträchtigen. Wer damit rechnen muss, dass seine Versammlungsteilnahme behördlich registriert wird und ihm dadurch Risiken entstehen können, wird möglicherweise auf die Ausübung der Versammlungsfreiheit verzichten, wodurch die individuellen Entfaltungschancen des Einzelnen beeinträchtigt werden.

Das Grundrecht auf Versammlungsfreiheit schützt deshalb die personenbezogenen Daten der Betroffenen bei der Vorbereitung von Versammlungen und während ihrer Durchführung vor staatlicher Ausspähung, beispielsweise durch Bild- und Tonaufnahmen, und damit möglicherweise bewirkter Einschüchterung (vgl. Dietel/Gintzel/Kniesel, Kommentar zum Gesetz über Versammlungen und Aufzüge, 13. Auflage, § 1 Rdnr. 80).

Ich habe deshalb das Polizeipräsidium München aufgefordert, während Versammlungen und Aufzügen in diesem Bereich die zur Überwachung des Hauptbahnhofvorplatzes und des Stachusrondells installierten polizeilichen Kameras abzuschalten und, wenn möglich, nach oben oder unten zu drehen.

Meiner im Zusammenhang mit der Videoüberwachung bereits seit langem erhobenen Forderung nach einer Evaluierung der Maßnahmen durch Auswertung der Kriminalitätszahlen für die Überwachungsgebiete sind die Polizeipräsidien in Nürnberg und Regensburg nachgekommen. Für den Bereich Regensburg wurde mir hierzu ein Bericht vorgelegt, aus dem sich ergibt, dass in der Zeit der Videoüberwachung an fast allen Örtlichkeiten eine zum Teil erhebliche Verringerung der Straftaten festzustellen war. Insbesondere im Bereich der Eigentums- und Betäubungsmittelkriminalität wies die Statistik einen erheblichen Rückgang auf. Darüber hinaus wurde mitgeteilt, dass eine Verdrängung der Kriminalität an andere Örtlichkeiten nicht erkennbar gewesen sei. Anders stellten sich jedoch die Erkenntnisse aus der Videoüberwachung in Nürnberg dar. In dem diesbezüglichen Erfahrungsbericht wird ausdrücklich angeführt, dass sich durch die Videoüberwachung keine signifikante Veränderung der Fallzahlen im videoüberwachten Raum ergeben haben, eine prozentuale Veränderung des Fallaufkommens im überwachten Raum zur Gesamtsituation in Nürnberg nicht erkennbar und eine Veränderung (Steigerung) der Aufklärungsquote auf den ersten Blick nicht festzustellen sei. Allerdings habe die Videoüberwachung zu einer erleichterten Aufklärung von Straftaten beigetragen.

Eine abschließende Aussage über die weitere Erforderlichkeit und die Geeignetheit der Videoüberwachung an den genannten Orten lässt sich aufgrund des relativ kurzen Beurteilungszeitraums noch nicht treffen. Ich halte es deshalb für notwendig, die Entwicklung weiter zu beobachten und in regelmäßigen Abständen zu bewerten.

7.13.2 Videoüberwachung des Wiesn-Geländes während des Oktoberfests

Seit der Wiesn 2002 sind in München auf dem Wiesn-Gelände an verschiedenen Standorten Kameras installiert, mit denen während des Oktoberfests personenbezogene Bildaufnahmen angefertigt werden (2002: 9 Standorte, 2003: 11 Standorte, 2004: 12 Standorte). Gegen die Durchführung dieser Videoüberwachung habe ich keine grundsätzlichen datenschutzrechtlichen Bedenken. Eine Statistik des Polizeipräsidiums München über die in den Jahren 1999 - 2001 während des Oktoberfests begangenen Straftaten zeigt, dass die gesetzlichen Voraussetzungen

(Art. 32 Abs. 2 PAG) für eine polizeiliche Videoüberwachung vorlagen.

Ich habe aber gefordert, dass auf die Videoüberwachung durch Schilder ausreichend hingewiesen wird. Allein eine „offensive Öffentlichkeitsarbeit", d.h. Berichte über die Videoüberwachung in den Medien, ist nicht ausreichend, um die Besucher des Oktoberfests über die Maßnahme zu informieren und die Videoüberwachung als „offene" Maßnahme erkennen zu lassen. Das Polizeipräsidium München hat meiner Forderung entsprochen und Hinweisschilder in deutscher und englischer Sprache angebracht.

Da die Videobänder erst zwei Monate nach Erstellung der Aufnahmen gelöscht werden, habe ich auch für die Aufbewahrung und Auswertung der Videobänder datenschutzrechtliche Vorkehrungen gefordert:

- Es sollte sichergestellt werden, dass nur namentlich genau bezeichnete Personen Zugriff auf die Videoaufzeichnungen mittels individuellem Passwort und eigener Benutzerkennung erhalten.

- Die Anzahl der Zugriffsberechtigten sollte unter dem Gesichtspunkt der Erforderlichkeit eng begrenzt sein.

- Nicht nur schriftliche, sondern auch telefonische Anfragen sollten protokolliert werden.

- Die Protokollierung sollte den Grund der Anfrage einschließlich des zugehörigen Aktenzeichens sowie die Name des anfragenden Polizeibeamten (nicht nur dessen Organisationseinheit) erkennen lassen.

- Es sollten nicht nur Datum und Uhrzeit des Zugriffs festgehalten werden, sondern auch, welche Aufzeichnungen eingesehen und ggf. vervielfältigt wurden.

Während für die ersten drei Punkte die erforderlichen Vorkehrungen getroffen wurden, ist das Polizeipräsidium München nicht bereit, den Grund der Abfrage sowie den Umfang der Einsichtnahme und ggf. der Vervielfältigung zu protokollieren. Eine weitergehende Protokollierungspflicht würde einen zusätzlichen Verwaltungsaufwand bedeuten und sei bei der voraussichtlich geringen Zahl der Abfragen entbehrlich. Ich habe angesichts der nur fragmentarischen Protokollierung - auch bei der zu erwartenden Quantität der Zugriffe - erhebliche Zweifel, ob eine ausreichende Nachvollziehbarkeit von Zugriffen gewährleistet ist. Ich beabsichtige, mich zu gegebener Zeit davon zu überzeugen.

7.14 Bild- und Tonaufnahmen von Versammlungsteilnehmern

In meinem letzten Tätigkeitsbericht (Nr. 6.14) hatte ich meinen Eindruck beschrieben, dass die Polizei entgegen den gesetzlichen Vorschriften bei Versammlungen auch vorsorglich Videoaufzeichnungen für den Fall anfertigt, dass sich zu einem späteren Zeitpunkt ein Straftatenverdacht ergeben sollte. Das Gesetz lässt jedoch Videoaufzeichnungen nur dann zu, wenn entweder ein Anfangsverdacht einer Straftat hinsichtlich der betroffenen Person besteht oder bei den betroffenen Versammlungsteilnehmern tatsächliche Anhaltspunkte dafür bestehen, dass gerade von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Um der Tendenz der vorsorglichen Anfertigung von Bildaufnahmen einer Vielzahl von Personen wegen zu erwartender Straftaten oder Gefahrenlagen entgegenzuwirken, habe ich wie angekündigt weitere Kontrollen durchgeführt.

Bei einer datenschutzrechtlichen Prüfung von umfangreichen polizeilichen Videoaufnahmen bei einer Versammlung im Rahmen der Sicherheitskonferenz 2003 habe ich Folgendes festgestellt:

Anlässlich einer großen Versammlung hatte die Polizei mehrere Videotrupps im Einsatz, von denen einige Videoaufzeichnungen zur Beweissicherung anfertigten, andere zur Dokumentation. Sämtliche Videobänder wurden von mir überprüft. Dabei habe ich festgestellt, dass die Beweissicherungsbänder zu einem großen Teil Übersichtsaufnahmen des Demonstrationsgeschehens enthielten. Es wurden jedoch immer wieder ohne erkennbaren Grund Personengruppen oder auch einzelne Personen herangezoomt. Hierdurch wurden die einzelnen Personen aus der Masse der Demonstranten hervorgehoben und erkennbar gefilmt, ohne dass hierfür eine gesetzliche Grundlage ersichtlich war. Von diesen Personen gingen weder Gefahren aus noch hatten sie Straftaten begangen.

Ich habe daher das zuständige Polizeipräsidium darauf hingewiesen, dass ein derartiges Heranzoomen und Filmen von einzelnen Personen und Personengruppen, durch die die Versammlungsteilnehmer personenbezogen erfasst werden, mit dem Gesetz nicht zu vereinbaren ist und gefordert, diese Praxis in Zukunft zu unterlassen.

Daneben habe ich festgestellt, dass auch zugbegleitende polizeiliche Videoaufzeichnungen vorgenommen wurden, bei denen sich der Kameramann meist direkt neben dem Demonstrationszug oder in dessen unmittelbarer Nähe befand, so dass sich die Aufzeichnungen ebenfalls nicht auf Übersichtsaufnahmen beschränkten. Auch hier wurden einzelne Personen oder Personengruppen individuell erkennbar

aufgezeichnet, ohne dass hierfür eine gesetzliche Grundlage vorhanden gewesen wäre. Gleiches gilt für die Aufnahmen durch die Dokumentationstrupps, die lediglich Schulungszwecken dienen sollten.

Insbesondere im Hinblick auf meine Ausführungen in früheren Fällen habe ich daher dem zuständigen Polizeipräsidium nahegelegt, eine intensive Belehrung der Verantwortlichen und möglicherweise auch eine Änderung des Filmkonzepts vorzunehmen. Das Polizeipräsidium hat sich einsichtig gezeigt, die Vernichtung der Videobänder zugesagt und mitgeteilt, dass es die Fachdienststellen beauftragt habe, die jeweils eingesetzten Beamten im Rahmen der Aus- und Fortbildung nochmals eingehend hinsichtlich der datenschutzrechtlichen Bestimmungen über Bildaufzeichnungen bei Versammlungen zu schulen. Hierdurch könnten die Beamten im Umgang mit datenschutzrechtlichen Bestimmungen sensibilisiert und fehlerhafte Verhaltensweisen künftig vermieden werden. Ob dieses Ziel erreicht wird, werde ich auch in Zukunft durch die Kontrolle von Videoaufzeichnungen von Versammlungen überprüfen.

7.15 Bildanfertigung von in Gewahrsam genommenen Personen

Im Rahmen einer Eingabe eines Bürgers wurde mir folgendes Vorgehen der Polizei anlässlich der Münchner Sicherheitskonferenz im Jahre 2003 bekannt:

Der Polizei lagen konkrete Anhaltspunkte dafür vor, dass sich an einer als Treffpunkt der linksextremistischen Szene bekannten Örtlichkeit Gegner der Münchner Sicherheitskonferenz treffen und dort Straftaten verabreden wollten. Daher führte die Polizei in der Örtlichkeit eine Kontrolle durch, in deren Rahmen sie bei sämtlichen angetroffenen Personen eine Identitätsfeststellung durchführte. Von den dergestalt überprüften Personen wurden 22 von der Polizei in Gewahrsam genommen und in diesem Zusammenhang auch fotografiert.

Zwar war die Identitätsfeststellung aller angetroffenen Personen nach Art. 13 PAG zulässig, da aufgrund der vorliegenden Informationen anzunehmen war, dass in der Örtlichkeit Straftaten verabredet bzw. vorbereitet wurden und darüber hinaus auch von einer konkreten Gefahr für die öffentliche Sicherheit und Ordnung ausgegangen werden konnte. Demgegenüber war die pauschale Anfertigung von Lichtbildern aller in Gewahrsam genommener Personen rechtwidrig. Es handelte sich hierbei um eine erkennungsdienstliche Maßnahme, deren Voraussetzungen nicht vorlagen.

Die Polizei hat mir auf meine Nachfrage mitgeteilt, die Sofortbilder hätten der „Beschleunigung des Verfahrens vor Ort“ und der „eindeutigen Zuordnung für die weitere polizeiliche Sachbearbeitung“ gedient. Dies sei aufgrund mangelnder Glaubwürdigkeit der Angaben der Betroffenen und mangelnder Aktualität der mitgeführten Legitimationsnachweise erforderlich. Die Polizei könne die Echtheit der Personaldokumente im Rahmen der Identitätsfeststellung vor Ort nicht im erforderlichen Umfang prüfen. Außerdem könnten die einzelnen Personen anhand des Lichtbilds den Vorgängen zweifelsfrei zugeordnet werden, wenn sie über ihre tatsächliche Identität falsche Angaben gemacht hätten.

Ich habe die Polizei darauf hingewiesen, dass diese Begründung keine pauschale erkennungsdienstliche Behandlung aller in Gewahrsam genommener Personen rechtfertigt. Nach Art. 14 Abs. 1 Nr. 1 PAG kann die Polizei erkennungsdienstliche Maßnahmen vornehmen, wenn eine nach Art. 13 PAG zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Wie sich auch aus der Vollzugsbekanntmachung zum Polizeiaufgabengesetz ergibt, kommt eine erkennungsdienstliche Maßnahme nach dieser Vorschrift nur in Betracht, wenn andere Möglichkeiten der Identitätsfeststellung mit zumutbarem Aufwand im Einzelfall nicht bestehen. Dies bedeutet, dass die Anfertigung eines Lichtbildes grundsätzlich dann nicht zulässig ist, wenn der Betroffene sich ausweisen kann. Etwas anderes kann nur dann gelten, wenn im konkreten Einzelfall Anhaltspunkte dafür bestehen, dass der vom Betroffenen vorgezeigte Personalausweis gefälscht oder auf eine andere Person ausgestellt ist bzw. wenn er nicht mehr gültig ist. Kann der in Gewahrsam Genommene aber einen noch gültigen, auf ihn ausgestellten Ausweis vorzeigen, bei dem keinerlei konkrete Anhaltspunkte für eine Fälschung bestehen, ist die Anfertigung eines Lichtbildes nicht zulässig. Demgegenüber hatte die Polizei pauschal alle in Gewahrsam genommenen Personen fotografiert, ohne Rücksicht darauf, ob sich unter diesen überhaupt solche befanden, die sich nicht ausweisen konnten oder bei denen konkrete Anhaltspunkte für eine Fälschung oder unberechtigte Nutzung des Ausweispapiers vorlagen. Die von der Polizei vorgetragenen allgemeinen Überlegungen, wie die Beschleunigung des Verfahrens oder die rein theoretische Möglichkeit von gefälschten Papieren, können keine erkennungsdienstliche Maßnahme rechtfertigen.

Ich habe daher die Polizei aufgefordert, diese rechtswidrige Verfahrensweise in Zukunft zu unterlassen. Die Polizei hat mir mitgeteilt, dass die angefertigten Lichtbilder gelöscht wurden und meine Rechtsauffassung künftig berücksichtigt wird.

7.16 Datenübermittlung an die Presse

Die Problematik der Übermittlung personenbezogener Daten durch die Polizei an die Medien hat mich auch in diesem Berichtszeitraum wieder beschäftigt. Dabei habe ich mehrmals feststellen müssen, dass solche Übermittlungen der Polizei der erforderlichen vorausgehenden Güter- und Interessenabwägung entbehrten, so dass die Persönlichkeitsrechte der Betroffenen zum Teil erheblich verletzt wurden. Gerade bei Äußerungen zu prominenten Persönlichkeiten, hat sich gezeigt, dass häufig kein legitimes Informationsinteresse der Öffentlichkeit besteht, sondern mit der Information lediglich der Sensationslust Rechnung getragen wird.

Durch einen Bürger wurde ich auf ein Radiointerview eines Polizeibeamten hingewiesen, in dem dieser anlässlich eines bekannt gewordenen Verkehrsunfalls einer bekannten Persönlichkeit auf Nachfrage mitteilte, dass auch zwei weitere, namentlich erwähnte prominente Persönlichkeiten im Bereich derselben Polizeidirektion an Verkehrsunfällen beteiligt gewesen seien. Ich habe die zuständige Polizeidienststelle darauf hingewiesen, dass diese Datenübermittlung unzulässig war, weil kein rechtliches Interesse an der Benennung prominenter früherer Unfallteilnehmer erkennbar war und zudem das schutzwürdige Interesse der Betroffenen an einer Geheimhaltung überwog. Das hiergegen von der Polizei vorgebrachte Argument, es liege keine polizeiliche Datenübermittlung vor, da nur eine in der Öffentlichkeit bereits bekannte Information erwähnt worden sei, habe ich zurückgewiesen. Auch auf Geschehnisse, die zu einem früheren Zeitpunkt öffentlich geworden sind, sind die Datenschutzvorschriften grundsätzlich anwendbar. Wenn die Polizei solche Informationen aufgrund polizeilicher Kenntnis bekannt gibt oder bestätigt, liegt eine Datenübermittlung vor, die nur unter den gesetzlichen Voraussetzungen zulässig ist.

In einer Tageszeitung wurde berichtet, dass gegen einen bekannten Schauspieler wegen des Verdachts des Ladendiebstahls ermittelt werde. Auf meine Nachfrage teilte das zuständige Polizeipräsidium mit, Mitarbeiter der Tageszeitung hätten den Vorfall bei der Pressestelle geschildert und angefragt, ob hierzu Erkenntnisse vorliegen. Dies sei lediglich bestätigt worden. Auch hier stellte sich die Polizei auf den Standpunkt, es habe keine Datenübermittlung an die Presse stattgefunden, da mangels eigeninitiativer bzw. weitergehender Übermittlung personenbezogener Daten keine über den Kenntnisstand der Presse hinausgehende Auskunft erteilt worden sei.

Dieser Rechtsauffassung bin ich entgegengetreten. Die Bestätigung eines bestimmten Vorfalls durch die Polizei stellt eine Datenübermittlung dar. Entscheidend hierfür ist die besondere Qualität der amtlichen Bestätigung durch die dafür zuständige Behörde. Bevor eine solche Bestätigung erteilt wird, handelt es sich lediglich um eine mehr oder weniger gesicherte Annahme. Gerade weil die Presse den Wahrheitsgehalt solcher Mitteilungen durch Dritte nicht mit Sicherheit beurteilen kann, fragt sie bei der Polizei nach, um sich vor einer Veröffentlichung abzusichern.

Auch bei absoluten und relativen Personen der Zeitgeschichte hat die Polizei für die Frage der Zulässigkeit einer Datenübermittlung an die Presse eine Abwägung der widerstreitenden Interessen, namentlich der Intensität des Eingriffs in die Persönlichkeit des Betroffenen, der Art und Schwere der Straftat, des Verdachtsgrads, der konkreten Stellung bzw. Tätigkeit des Betroffenen sowie des Auskunftsanspruchs der Presse, vorzunehmen. Bei diesen Personen muss bei der Abwägung berücksichtigt werden, dass nur ein legitimes Informationsinteresse der Öffentlichkeit erheblich ist, nicht jedoch bloße Neugier oder Sensationslust. Bei bekannten Persönlichkeiten besteht nämlich die Besonderheit, dass das Interesse der Öffentlichkeit an ihnen unabhängig vom konkreten Tatvorwurf regelmäßig besonders groß ist. Dieses besondere Interesse ist aber nur dann berechtigt bzw. legitim, wenn die Straftat einen Bezug zur Stellung bzw. Tätigkeit der Persönlichkeit hat. In diesem Fall ist grundsätzlich nicht die Schwere der Straftat entscheidend, vielmehr muss die konkrete Stellung bzw. Tätigkeit des Betroffenen im Zusammenhang mit der Straftat beurteilt werden. Dabei kann sich auch bei leichteren Straftaten ein legitimes Informationsinteresse der Öffentlichkeit ergeben, so z.B. wenn ein Justizminister oder Polizeipräsident eines Ladendiebstahls verdächtigt würde. Aufgrund des Bezugs zwischen der vorgeworfenen Straftat und dem Amt und der damit verbundenen Glaubwürdigkeit des Amtsinhabers bestünde hier grundsätzlich ein legitimes Interesse der Öffentlichkeit an der Unterrichtung.

Ausgehend von diesen Grundsätzen war in o.a. Fall die Bestätigung des Ermittlungsverfahrens wegen Ladendiebstahls gegen einen bekannten Schauspieler unzulässig. Gegenstand des Tatvorwurfs war ein geringfügiges Delikt, dessen evtl. Begehung keinen Einfluss auf die Glaubwürdigkeit des Betroffenen in seinem Beruf, wohl aber auf seine Reputation in der Öffentlichkeit haben konnte. Ein legitimes Informationsinteresse der Öffentlichkeit - noch dazu im Stadium der Ermittlungen, vor Anklageerhebung oder Verurteilung - lag deshalb nicht vor.

In einem weiteren Fall hatte sich eine Bürgerin an mich gewandt, weil in einer Fernsehsendung personenbezogene Daten zu ihrer Person sowie Informationen zu gegen sie gerichteten Ermittlungs- und laufenden Gerichtsverfahren gesendet worden seien. Ich habe mir daraufhin von der Polizei eine Videoauf-

zeichnung über den Sendebeitrag zuschicken lassen. Darin wurde die Petentin im Rahmen einer Berichterstattung über „Okkultismus“ von Nahem gefilmt und interviewt, außerdem wurde ihr Vorname erwähnt. Im Rahmen des Beitrags gab zudem ein Polizeibeamter mehrfach Stellungnahmen zu den gegen die Petentin erhobenen Vorwürfen sowie zu weiteren, nicht mit dem Fall in direktem Zusammenhang stehenden polizeilichen Erkenntnissen ab. Auch in diesem Fall vertrat das Polizeipräsidium die Auffassung, es habe mangels eigener Namensnennung durch die Polizei keine Datenübermittlung an die Presse vorgelegen. Erst durch die abschließende Gestaltung in Form des Zusammenschnitts aller Interviews sei der Anschein einer Datenübermittlung entstanden.

Diese Auffassung ist nicht zutreffend. Dem Polizeibeamten war aufgrund von vorgelegten Unterlagen bereits vor seinem Interview bewusst, dass die Petentin den Reportern namentlich bekannt ist. Jede Information, die der Beamte den Reportern über den Fall und die Beschuldigte zugänglich machte, konnte daher von diesen eindeutig auf die namentlich bekannte Petentin bezogen werden und stellt damit eine Datenübermittlung an die Presse dar. Dabei spielt es keine Rolle, dass der Beamte selbst in seinem Interview den Namen der Petentin nicht erwähnte, sondern diese nur als „Dame“ bezeichnet hatte, da alle Gesprächspartner wussten, wer damit gemeint war. Der spätere Zusammenschnitt durch die Reporter und die entsprechende Fernsehübertragung bewirkten zusätzlich, dass die Datenübermittlung der Polizei einem größeren Personenkreis zugänglich gemacht wurde. Damit musste die Polizei aufgrund der Anfrage sowie der Aufgabe und Funktion der Presse auch rechnen.

Wegen des weit überwiegenden Geheimhaltungsinteresses der Petentin hätte die Polizei keine Datenübermittlung vornehmen dürfen. Angesichts des schwerwiegenden Eingriffs in das Recht auf informationelle Selbstbestimmung der Petentin durch die Übermittlung ihrer personenbezogenen Daten habe ich diesen Datenschutzverstoß gemäß Art. 31 Abs. 1 BayDSG förmlich beanstandet.

7.17 Reality TV

Auf die datenschutzrechtliche Problematik der Zusammenarbeit von Polizei und Presse bei der Produktion von Sendungen über polizeiliche Einsätze bin ich bereits in meinem letzten Tätigkeitsbericht (Nr. 6.20) eingegangen. Ausgehend von den Grundsätzen, die ich in meinem letzten Tätigkeitsbericht dargestellt hatte, hat sich das Staatsministerium des Innern mit der Thematik befasst. Es hat zwischenzeitlich zur Gewährleistung einer einheitlichen und praxisgerechten Handhabung bei der bayerischen Polizei eine interne Richtlinie für die Zusammenarbeit von Polizei und Presse bei der Produktion von Sendungen über polizeiliche Einsätze erlassen, die in einem intensiven Gedankenaustausch mit mir abgestimmt wurde. Darin wird zwischen sog. „Reality-Reportagen“, die ausschließlich im Interesse der Presse liegen und keinen Bezug zu polizeilicher Öffentlichkeitsarbeit haben, und der Ermöglichung der Berichterstattung durch die Polizei unterschieden. Während erstere nach der Richtlinie stets unzulässig sind, gelten für die Berichterstattung nun folgende Grundsätze:

Personen dürfen grundsätzlich erkennbar erst dann gefilmt werden, wenn sie zuvor in die Aufnahmen eingewilligt haben. Die Einwilligung des Betroffenen ist dabei nur wirksam, wenn er vorher über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufgeklärt und hierbei auf die Freiwilligkeit seiner Einwilligung hingewiesen wurde. Soweit dies möglich ist, sollte die Einwilligung schriftlich eingeholt werden, andernfalls ist sie anderweitig zu dokumentieren. Entsprechend meiner Forderung muss der Dokumentation neben dem Inhalt der Aufklärung auch zu entnehmen sein, inwieweit sich die Einwilligung neben der Aufnahme auch auf die Ausstrahlung erstreckt. Sofern das Filmmaterial für einen anderen Beitrag verwendet werden soll, ist eine erneute Einwilligung des Betroffenen einzuholen, es sei denn, dass das Einverständnis hierzu bereits bei der Einwilligung zur Bildaufzeichnung erteilt wurde.

Verweigert eine Person die vorherige Einwilligung, darf sie nicht gefilmt werden. Bis zur Erteilung der Einwilligung sollten nur Übersichtsaufnahmen angefertigt werden, die den Betroffenen nicht individuell erkennen lassen. Sind im Rahmen von Übersichtsaufnahmen dennoch Personen vor deren Einwilligung erkennbar gefilmt worden, so ist deren Einwilligung nachträglich einzuholen. Verweigern die Betroffenen ihre nachträgliche Einwilligung, so ist das angefertigte personenbezogene Filmmaterial unverzüglich zu vernichten bzw. zu löschen oder der Polizei zum Zwecke der Löschung zu überlassen. Auf meine Anregung wurde die Richtlinie in diesem Punkt noch dahin gehend ergänzt, dass ein Rückgriff auf die gesetzliche Regelung der Datenübermittlung an Private dann nicht möglich ist, wenn der Betroffene seine vorherige Einwilligung verweigert, so dass in diesem Fall die Presse von personenbezogenen Bild- und Filmaufnahmen Abstand zu nehmen hat.

Diese Richtlinie begrüße ich. Ich meine, dass den Interessen des Betroffenen dadurch ausreichend Rechnung getragen wird.

7.18 Meldung suchtkranker oder suchtgefährdeter Personen an die Gesundheitsämter

Das Staatsministerium für Gesundheit, Ernährung und Verbraucherschutz ist mit der Bitte an mich herangetreten, die Frage der Meldung von suchtkranken oder suchtgefährdeten Personen von der Polizei an die Gesundheitsämter im Hinblick auf das zum 01.01.2001 in Kraft getretene Infektionsschutzgesetz (IfSG) zu beurteilen. Nach einer aus dem Jahr 1996 stammenden und auf der damaligen Rechtslage beruhenden Richtlinie des Staatsministerium des Innern hatte die Polizei ihr bekannt gewordene suchtkranke oder suchtgefährdete Personen stets an das Gesundheitsamt zu melden, um diesem die Suchtkrankenfürsorge und Seuchenbekämpfung zu ermöglichen. Nachdem mit dem Erlass des Infektionsschutzgesetzes die seuchenrechtlichen Pflichtuntersuchungen entfallen sind, hielten einige Gesundheitsämter die Beibehaltung der pauschalen Datenübermittlungen durch die Polizei für entbehrlich, während andere weiterhin auf die genannten Personen zugingen und eine Untersuchung anboten. Die Staatsministerien des Innern sowie für Gesundheit, Ernährung und Verbraucherschutz vertraten hierzu die Auffassung, der primäre Aspekt der Suchtkrankenfürsorge sei nur durch die polizeiliche Datenübermittlung der betreffenden Personen an die Gesundheitsbehörden möglich.

Ich habe das Staatsministerium für Gesundheit, Ernährung und Verbraucherschutz darauf hingewiesen, dass nach Inkrafttreten des Infektionsschutzgesetzes eine pauschale Datenweitergabe der Namen von suchtkranken oder suchtgefährdeten Personen durch die Polizei an die Gesundheitsämter mit den Bestimmungen des Datenschutzes nicht mehr vereinbar 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. Die Kenntnis sämtlicher suchtkranker oder suchtgefährdeter Personen ist aber nach der Rechtsänderung zur Erfüllung der Aufgaben nicht mehr erforderlich, da zugunsten einer möglichst frühzeitigen Beratung auf freiwilliger Basis auf Zwangsuntersuchungen oder -beratungen verzichtet wird. Somit kommt nur noch die Übermittlung der Daten derjenigen Personen in Betracht, bei denen es aus der Sicht der Polizei im Einzelfall aufgrund bestimmter Umstände möglich erscheint, dass das Gesundheitsamt bestimmte Anordnungen treffen kann, weil Erkenntnisse darüber vorliegen, dass diese Personen durch ihr Verhalten Gesundheit oder Leben anderer gefährden.

Darüber hinaus bin ich auch der Argumentation entgegengetreten, die namentliche Kenntnis von Suchtkranken sei für die Gesundheitsbehörden auch zum Vollzug des Unterbringungsgesetzes unabdingbar. Diesbezüglich habe ich darauf hingewiesen, dass nicht die Gesundheitsämter, sondern die Kreisverwaltungsbehörden für den Antrag im Unterbringungsverfahren zuständig sind. Liegen Anhaltspunkte für die Notwendigkeit einer Unterbringung vor, darf die Polizei daher lediglich die Kreisverwaltungsbehörde unterrichten, die dann ihrerseits über die Einbindung des Gesundheitsamts entscheidet.

Das Staatsministerium des Innern hat die Richtlinie zur Meldung suchtkranker oder suchtgefährdeter Personen durch die Polizei an die Gesundheitsämter entsprechend meinen Ausführungen geändert. Dabei hat es zutreffend darauf hingewiesen, dass es darauf ankommt, dass die zu übermittelnden Daten für die Aufgaben des Gesundheitsamts aus der Sicht der Polizei erforderlich erscheinen, während die endgültige Klärung der Frage, ob die Person durch ihr Verhalten Gesundheit und Leben anderer gefährdet und daher eine Anordnung zulässig ist, vom Gesundheitsamt vorgenommen wird.

7.19 Abfragen im polizeilichen Informationssystem

Auch in diesem Berichtszeitraum waren - wie in den zwei vorangegangenen - wieder problematische Abfragen im polizeilichen Informationssystem festzustellen, die das soziale Umfeld der abfragenden Polizeibediensteten betrafen. Wie in meinem 20. Tätigkeitsbericht ausgeführt (vgl. Nr. 6.25), hat das Innenministerium die von mir vorgeschlagenen Maßnahmen zur Verbesserung des Schutzes gegen die Gefahr des Missbrauchs interner (polizeilicher) Daten für private Zwecke (z.B. Einbindung eines Vorgesetzten vor der Datenabfrage) abgelehnt. Die nachfolgenden Beispiele zeigen deutlich die Gefahren:

Eine Bürgerin hatte sich an mich gewandt, da sie eine im privaten Interesse durchgeführte Abfrage ihrer personenbezogenen Daten durch einen Polizeibeamten vermutete, der gleichzeitig ihr Vermieter war. Eine von mir veranlasste Auswertung des Protokollbestandes der Polizei ergab, dass der betreffende Polizeibeamte personenbezogene Daten der Petentin im Einwohnermeldeverfahren (EWO) abgefragt hatte. Das zuständige Polizeipräsidium teilte mir auf Anfrage mit, dass die betreffenden Datenabfragen von dem Polizeibeamten von dessen dienstlichem Arbeitsplatz auf Grund des von der Petentin vermuteten privaten Anlasses (Mietverhältnis) durchgeführt worden waren.

Der Datenabgleich mit dem Bestand des Einwohnermeldeverfahrens ist nach dem Bayerischen Meldegesetz nur zulässig, wenn im Einzelfall die Kenntnis der Daten zur Erfüllung polizeilicher Aufgaben erforderlich ist. Des Weiteren ist geregelt, dass der Empfänger der Daten diese nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt worden sind. Das Informationsinteresse des Beamten hatte sich aber aus seiner privaten Stellung als Wohnungsvermieter ergeben. Der Datenabgleich und die Datennutzung, die zu privaten Zwecken erfolgten, waren deshalb unzulässig. Ich habe die Polizei aufgefordert darauf hin zu wirken, dass künftig solche datenschutzrechtlichen Verstöße vermieden werden.

In einem ähnlichen Fall hatte ein Polizeibeamter ein Fahrzeug über das Zentrale Verkehrsinformationssystem (ZEVIS) zur Feststellung des Halters abgefragt. Die Abfrage stand im Zusammenhang mit einem Rechtsstreit auf Grund des Mietverhältnisses zwischen dem Polizeibeamten und der Fahrzeugführerin. Diese hatte Prozesskostenhilfe beantragt, wobei der abfragende Beamte als Beklagter vom zuständigen Amtsgericht zur Stellungnahme aufgefordert worden war. Nach seinen Angaben habe er im Hinblick auf ein von der Mieterin geführtes Kfz mit ortsfremden Kennzeichen einen Betrug durch Verschleierung der Vermögensverhältnisse vermutet und deshalb eine Halterabfrage durchgeführt. Zwar ist eine solche Abfrage nach dem Straßenverkehrsgesetz zur Verfolgung von Straftaten zulässig. Jedoch war offensichtlich, dass sich das Informationsinteresse des Beamten aus der Vermischung privater Interessen als Hausvermieter bzw. Prozessbeklagter und möglichen dienstlichen Interessen als Hilfsbeamter der Staatsanwaltschaft ergeben hat. Der Fall macht deutlich, dass vor dienstlichen Ermittlungen im sozialen Umfeld des Polizeibeamten, noch dazu wenn seine eigenen Interessen berührt sind, eine innerdienstliche Überprüfung durch den Vorgesetzten und die Abgabe des Vorganges an einen nicht befangenen Beamten grundsätzlich notwendig sind.

In einem anderen Fall vermutete eine Bürgerin eine unzulässige Datenabfrage und Datenübermittlung ihrer Halterdaten aus dem Fahrzeugregister an eine Privatperson durch einen Polizeibeamten, nachdem ihr ein entsprechender E-Mail-Schriftverkehr zwischen dem Beamten und einer Privatperson bekannt geworden war. Darin hatte der Beamte dem offenbar befreundeten Empfänger mitgeteilt, dass das Fahrzeug der Petentin noch unter einer früheren Wohnanschrift angemeldet war. Eine von mir veranlasste Protokolldateiauswertung beim LKA ergab, dass die personenbezogenen Daten der Petentin von einem Polizeibeamten im Zentralen Verkehrsinformationssystem (ZEVIS) abgefragt worden waren. Der Beamte hat die unzulässige Datenabfrage und -übermittlung zwischenzeitlich eingeräumt. Eine innerdienstliche Überprüfung der Angelegenheit im Hinblick auf evtl. straf-, bußgeld- bzw. disziplinarrechtliche Konsequenzen wurde eingeleitet.

Wegen der Gefahr zukünftiger unzulässiger Abfragen aus privaten Motiven halte ich neben den von mir vorgeschlagenen Verbesserungsmaßnahmen auch die Durchführung der im Jahr 1998 vom Staatsministerium des Innern angeordneten anlassunabhängigen Auswahlprüfung von Datenabfragen für unerlässlich. Diese sollte sich allerdings nicht auf Abfragen des KAN-Bestandes beschränken.

7.20 Entbindung von der Schweigepflicht im Strafverfahren

In meinem letzten Tätigkeitsbericht (Nr. 6.18) hatte ich auf meine Bedenken gegen das bei der bayerischen Polizei verwendete Formblatt „Einwilligung zur Weitergabe personenbezogener Daten“ hingewiesen, durch dessen Unterzeichnung sowohl Geschädigte und Zeugen als auch Beschuldigte bestimmte Behörden oder sonstige Stellen (z.B. Arzt, Krankenkasse, Arbeitsamt, Finanzamt) gegenüber den Ermittlungsbehörden von der Schweigepflicht entbinden bzw. zur Weitergabe personenbezogener Daten ermächtigen. Zwischenzeitlich wurde ich über die beabsichtigte Verwendung des Formblatts auch in Ordnungswidrigkeitenverfahren in Kenntnis gesetzt.

Ich habe das Staatsministerium des Innern darauf hingewiesen, dass die Anwendung des Formblatts in Ordnungswidrigkeitenverfahren noch wesentlich stärkeren Bedenken begegnet, als die Anwendung im Strafverfahren. Ich halte es schon für bedenklich, wenn in besonders sensiblen und gesetzlich besonders geschützten Bereichen, in denen es um die Entbindung von beruflichen Schweigepflichten geht, die Datenerhebung nicht auf die gesetzlichen Eingriffsbefugnisse des Ordnungswidrigkeitengesetzes sondern auf die Einwilligung des Betroffenen gestützt werden soll. Im Hinblick darauf kommt der umfassenden und eindeutigen Aufklärung des Betroffenen, die Voraussetzung für eine wirksame Einwilligung ist, besondere Bedeutung zu. Die Hinweise auf dem Formblatt erwecken aber den unzutreffenden und irreführenden Eindruck, dass die Daten, für die die Einwilligung zur Weitergabe erklärt wird, in einem umständlicheren, langwierigeren und belastenderen Verfahren auch ohne diese Einwilligung von der Polizei erhoben werden könnten und die Einwilligung lediglich einer Beschleunigung und Vereinfachung des Verfahrens diene. Gerade durch den Hinweis, dass „im Einzelfall die Einholung richterlicher Anordnungen sowie die Notwendigkeit von Durchsuchungs- und Beschlagnahmemaßnahmen entfällt“ wird der Eindruck erweckt, die Polizei könne die erforderlichen Informationen auch ohne Zustimmung

des Betroffenen mittels richterlicher Anordnung erheben. Dies ist jedoch bei Ordnungswidrigkeitenverfahren sogar in der Mehrzahl der Fallkategorien unzutreffend.

Ich habe deshalb das Staatsministerium des Innern aufgefordert, die Anwendung des Formblatts gerade in Ordnungswidrigkeitenverfahren, bei denen es nicht um strafrechtlich relevantes Verhalten sondern nur um sog. Verwaltungsunrecht geht, aus datenschutzrechtlichen Gründen zu unterlassen. Dieses hat mir zugesagt, von einer Verwendung des Formblatts im Ordnungswidrigkeitenverfahren abzusehen.

7.21 Auskunft über präventive Speicherungen bei laufenden Ermittlungsverfahren

In meinem letzten Tätigkeitsbericht (Nr. 6.23) hatte ich die Problematik der Auskunftserteilung über präventivpolizeiliche Daten bei laufenden Ermittlungsverfahren dargestellt. Ich hatte darauf hingewiesen, dass - im Gegensatz zur Auffassung des Staatsministeriums des Innern - die Polizei als speichernde Stelle dieser Daten und nicht die Staatsanwaltschaft gegenüber dem Bürger für die Entscheidung über seinen Antrag auf Auskunftserteilung zuständig ist.

Nach der zwischenzeitlich mit dem Staatsministerium des Innern erzielten Einigung bezüglich der Auskunftserteilung über die im Kriminalaktennachweis auf der Grundlage präventiv polizeilicher Befugnisse gespeicherten Daten laufender Ermittlungsverfahren an den Betroffenen ist von der Polizei behördenintern stets die Entscheidung der zuständigen Staatsanwaltschaft als Herrin des Ermittlungsverfahrens herbeizuführen. Sofern die Staatsanwaltschaft zu dem Ergebnis kommt, dass die Auskunftserteilung aus Gründen der Gefährdung des Ermittlungsverfahrens abzulehnen ist, ist die Polizei an diese Entscheidung gebunden. Als speichernde Stelle ist sie aber selbst für die ggf. erforderliche Ablehnung des Antrags gegenüber dem Bürger zuständig. Eine Verweisung des anfragenden Bürgers an die Staatsanwaltschaft kommt nicht in Betracht.

§ 491 StPO regelt die Auskunftserteilung an Betroffene im Rahmen eines Ermittlungsverfahrens. Diese Vorschrift wurde durch das Gesetz zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften ergänzt. § 491 Abs. 1 StPO sieht nun vor, dass über Ermittlungsverfahren, deren Einleitung im Zeitpunkt der Beantragung der Auskunft noch nicht mehr als sechs Monate zurückliegt, keine Auskunft erteilt wird. Diese Frist kann im Einzelfall verlängert werden. Diese Ergänzung wird sich auch auf die Auskunftserteilung über präventivpolizeiliche Daten bei laufenden Ermittlungsverfahren auswirken.

7.22 Generelle Auskunftsablehnung bei Betäubungsmittelhandel

Nach Art. 48 Abs. 2 Nr. 1 PAG unterbleibt die Auskunft an den Betroffenen über die zu seiner Person gespeicherten Daten, soweit eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei, zu besorgen ist. Im Hinblick auf diese Regelung hatte das Staatsministerium des Innern festgelegt, dass in allen Fällen des unbefugten Rauschgifthandels eine Auskunft unterbleibt. In meinem letzten Tätigkeitsbericht (Ziffer 6.24) hatte ich darauf hingewiesen, dass diese Verfahrensweise mit der gesetzlichen Regelung nicht in Einklang steht. Die Ablehnung der Auskunftserteilung ist nur ausnahmsweise und nur nach Prüfung und Beurteilung des Einzelfalls zulässig.

Nach langwierigen Verhandlungen mit dem Staatsministerium des Innern hat dieses einen erneuten Verfahrensvorschlag vorgelegt:

Im Unterschied zu den bisherigen Vorschlägen wird darin erstmals dem aus datenschutzrechtlicher Sicht entscheidenden Erfordernis Rechnung getragen, dass in den Fällen des unbefugten Rauschgifthandels keine pauschale Entscheidung zu treffen ist, sondern eine Einzelfallprüfung durch die Polizeidienststelle zu erfolgen hat. Dabei sei allerdings davon auszugehen, dass bei der Betäubungsmittelkriminalität eine deliktsspezifisch eng verflochtene Händler- und Konsumentenstruktur vorhanden sei und deshalb im Zweifel von einer Ausforschungsgefahr auszugehen sei und eine Auskunft zu unterbleiben habe.

Wann ein derartiger Zweifelsfall anzunehmen ist, bleibt offen. In der überwiegenden Zahl der Fälle wird die Polizei keine Erkenntnisse darüber haben, ob der Auskunftsbegehrende Teil der kriminellen Strukturen der Szene ist. Dies gilt insbesondere dann, wenn bei der Polizei nur eine einzige Speicherung wegen Betäubungsmittelhandels zu einer ansonsten polizeilich nicht näher bekannten Person besteht. In diesen Fällen, in denen der Polizei keine näheren Erkenntnisse vorliegen, erscheint es nicht gerechtfertigt, aufgrund allgemeiner Überlegungen von Zweifeln auszugehen und die Auskunft zu verweigern. Ich habe deshalb im Interesse einer echten Verbesserung des polizeilichen Auskunftsverhaltens vorgeschlagen, dass nicht schon „im Zweifel“ von einer Ausforschungsgefahr ausgegangen werden müsse, sondern erst bei Vorliegen „entsprechender Anhaltspunkte“. Dies wurde vom Staatsministerium des Innern mit dem Hinweis abgelehnt, die besondere Problematik bei der Auskunftserteilung bei Fällen des unbefugten Rauschgifthandels bestehe gerade darin, dass der Polizei in zahlreichen Fällen gerade noch keine entsprechenden Anhaltspunkte vorliegen und aufgrund

der Besonderheiten dieses Deliktsbereichs eine erheblich erhöhte Ausforschungsgefahr bestehe.

Im Hinblick darauf, dass der Vorschlag des Staatsministeriums des Innern meiner grundlegenden Forderung nach einer Einzelfallprüfung durch die Polizei Rechnung trägt, habe ich meine nach wie vor bestehenden Bedenken zugunsten einer probeweise Einführung der vorgeschlagenen Regelung zurückgestellt. Zur Sicherstellung der datenschutzrechtlichen Überprüfung der konkreten Umsetzung dieser Regelung habe ich jedoch darum gebeten, die Polizeidienststellen aufzufordern, die Auskunftsvorgänge, die Speicherungen wegen Betäubungsmittelhandels betreffen, so vorzuhalten, dass sie ohne aufwendige Suche vorgelegt und von mir überprüft werden können. Da erst die praktischen Erfahrungen zeigen werden, wann die Polizeidienststellen von „Zweifeln" ausgehen und keine Auskunft erteilen, beabsichtige ich, nach einer einjährigen Erprobungsphase die polizeiliche Praxis der Auskunftserteilung in Fällen des Betäubungsmittelhandels zu überprüfen.

8 Verfassungsschutz

Beim Landesamt für Verfassungsschutz (LfV) habe ich im Berichtszeitraum wieder Überprüfungen von Datenerhebungen, -speicherungen und –übermittlungen sowie Auskunftserteilungen bzw. -ablehnungen durchgeführt. Die Prüfungen erfolgten anlassunabhängig (2 Prüfungen vor Ort) oder aufgrund von Bürgereingaben.

Des Weiteren habe ich die Änderung von Errichtungsanordnungen überprüft. Das Landesamt hat mich stets rechtzeitig beteiligt und meine datenschutzrechtlichen Hinweise weitgehend berücksichtigt. Zu weiteren für die nächste Zeit geplanten Vorhaben, die Auswirkungen auf den Datenschutz haben, wie bspw. die Modifizierung des Informationssystems IBA oder die Errichtung einer gemeinsamen bundesweiten Datei von Verfassungsschutz und Sicherheitsbehörden für den Bereich des islamistischen Terrorismus habe ich mich bereits geäußert (vgl. Nr. 8.6) und werde die weitere Entwicklung aufmerksam verfolgen.

8.1 Wohnraumüberwachung durch das Landesamt für Verfassungsschutz

Das Urteil des Bundesverfassungsgerichts vom 03.03.2004 zum Großen Lauschangriff ist auch für die verdeckte Datenerhebung durch das Landesamt für Verfassungsschutz von Bedeutung (vgl. auch Nr. 7.11), insbesondere für den Einsatz besonderer technischer Mittel zur Informationsgewinnung in Wohnungen. Notwendig ist deshalb eine Neufassung des Art. 6 a Bayerisches Verfassungsschutzgesetz (BayVSG), die die vom Bundesverfassungsgericht zum Schutz des Kernbereichs privater Lebensgestaltung aufgestellten Grundsätze beachtet. Diese gelten auch und gerade bei der Tätigkeit des Landesamts für Verfassungsschutz, dessen Aufgabe es ist, bereits im Vorfeld konkreter Straftaten beobachtend tätig zu werden.

Wenn schon das Landesamt für Verfassungsschutz aus übergeordneten Gründen des Allgemeinwohls im Vorfeld tätig werden darf, ist es umso wichtiger, den vom Bundesverfassungsgericht geforderten Grundrechtschutz zu gewährleisten, da Vorfeldtätigkeit auch einer erhöhten Gefahr der Fehlbeurteilung ausgesetzt ist. Dieser Schutz gilt grundsätzlich absolut und darf nicht durch Abwägung mit den staatlichen Interessen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden. Jeder Mensch muss zur Entfaltung seiner Persönlichkeit im Kernbereich privater Lebensgestaltung die Möglichkeit eines von staatlichen Stellen unbewachten Bereichs haben.

In diesem Sinne habe ich dem Staatsministerium des Innern die Grundzüge für eine Anpassung des Art. 6 a Abs. 1 BayVSG an die verfassungsrechtlichen Erfordernisse dargelegt. Im Einzelnen habe ich dabei auf Folgendes hingewiesen:

- Die Eingriffsvoraussetzungen des Art. 6 a Abs. 1 BayVSG mit ihren Verweisungen auf andere Gesetze und Strafvorschriften sind so zu fassen, dass sie dem Grundsatz der Normenklarheit entsprechen. Bei Ermächtigungen für Überwachungsmaßnahmen verlangt das Bestimmtheitsgebot, dass die betroffene Person erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist.

- Als Anknüpfungspunkt für den Eingriff sollte ein eigener, geschlossener und enger Straftatenkatalog entworfen werden. Eine pauschale Verweisung auf § 3 Abs. 1 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) und auf § 100 a Strafprozessordnung (StPO), die Straftaten mit unterschiedlichem Unrechtsgehalt aufweisen, halte ich nicht für ausreichend.

- Art. 6 a Abs. 1 BayVSG ist um eine Schutzvorschrift zugunsten von Gesprächen mit besonderen Vertrauenspersonen zu ergänzen, worunter auch Berufsgeheimnisträger nach § 53 StPO fallen.

- Die Übermittlungsmöglichkeit personenbezogener Daten an andere öffentliche Stellen ist einzuschränken. Sie darf nur zur Abwehr dringender Gefahren erfolgen, wie es Art. 13 Abs. 4 GG vorsieht. Außerdem darf eine Übermittlung nur zur Verfolgung solcher Straftaten gestattet werden, die besonders schwer sind.

- Die von der Maßnahme Betroffenen sind grundsätzlich nach Abschluss der Maßnahme zu benachrichtigen. Eine Zurückstellung der Benachrichtigung muss in angemessenen Zeitabständen gerichtlich überprüft werden.

- Die erlangten Daten müssen zur Sicherstellung der besonderen Zweckbindung gekennzeichnet werden.

- Die Anordnung sollte auf höchstens vier Wochen befristet werden.

Das Staatsministerium des Innern zeigte sich in der Sache grundsätzlich aufgeschlossen. Es teilte mit, dass es in vielen Punkten mit dem Ergebnis meiner vorläufigen Prüfung übereinstimme und hat gemäß Beschluss des Landtags vom 17.06.2004 diesem über die Auswirkungen der Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff auf die präventive Wohnraumüberwachung auch im Hinblick auf die Notwendigkeit von Änderungen des Bayerischen Verfassungsschutzgesetzes berichtet. Dabei vertritt es allerdings auch die Auffassung, dass dieses Urteil nicht voll inhaltlich auf das Gefahrenabwehrrecht zu übertragen sei. Dies halte ich, insbesondere bei Abweichungen von den Beschränkungen bezüglich des Deliktskatalogs, für bedenklich.

Ergänzend habe ich darauf hingewiesen, dass sich aus den Entscheidungen des Bundesverfassungsgerichts vom 03.03.2004 auch eine Prüfungs- und ggf. Anpassungsverpflichtung für die sonstigen verdeckten Datenerhebungsmaßnahmen nach dem Bayerischen Verfassungsschutzgesetz ergeben kann. Das Innenministerium teilt diese Auffassung offenbar nicht, da es auf die Eingriffsintensität der Maßnahme als solche, nicht auf den notwendigen Schutz des unantastbaren Kernbereichs privater Lebensgestaltung abstellt.

8.2 Datenschutzrechtliche Prüfungen beim Verfassungsschutz

Schwerpunkte meiner Prüfungen im Bereich des Verfassungsschutzes waren:

- Allgemeine Kontrolle von Dateien, Karteien und Akten
- Prüfung von Errichtungsanordnungen und internen Arbeitsanweisungen
- Prüfung von Datenerhebungen
- Bürgereingaben

Dabei habe ich festgestellt, dass das Landesamt für Verfassungsschutz die datenschutzrechtlichen Bestimmungen bei der Erhebung und Verarbeitung personenbezogener Daten grundsätzlich beachtet. Einzelne Fehler habe ich z.B. bei der Festsetzung von Speicherfristen und bei der Speicherung von Daten in Sachakten, die von der Polizei an das Landesamt übermittelt worden waren, festgestellt.

8.3 Speicherungen von „einfachen“ Mitgliedern

Unabhängig von meinen datenschutzrechtlichen Bedenken hinsichtlich der generellen Speicherung der Daten „einfacher“ Mitglieder extremistischer Gruppierungen in den Informationssystemen IBA bzw. NADIS, die ich bereits im Rahmen der Überarbeitung der hierfür geltenden Arbeitsanweisung im Jahre 1998 geltend gemacht habe, habe ich eine Überprüfung der Speicherungsgrundlagen für diesen Personenkreis vorgenommen. Durchgreifende Zweifel an der Mitgliedschaft der Betroffenen bei einer extremistischen Gruppierung hatte ich - abgesehen von einzelnen Ausnahmefällen - nicht. Jedoch habe ich das Landesamt für Verfassungsschutz aufgefordert, im Interesse einer besseren Überprüfungs- und Bewertungsmöglichkeit der Authentizität der Speicherungsgrundlage verstärkt dafür Sorge zu tragen, dass bei Mitgliederlisten Herkunft, Beschaffungsweise und Quelleneinstufung dokumentiert werden. Das Landesamt will dies für die Zukunft berücksichtigen.

Soweit der erforderliche Aktenrückhalt nicht (mehr) vorhanden war bzw. die Speichervoraussetzungen aus meiner Sicht nicht vorlagen, habe ich das Landesamt zur Löschung der Speicherungen aufgefordert. Diesen Forderungen ist das Landesamt umgehend nachgekommen.

8.4 Erforderlichkeitsprüfung bei Wiedervorlageterminen

Nach den Arbeitsanweisungen für die Speicherung und Löschung personenbezogener Daten zur Extremismusbeobachtung und zur Spionageabwehr muss grundsätzlich bei allen Speicherungen in den Auskunftssystemen IBA und NADIS nach Ablauf einer Wiedervorlagefrist die Erforderlichkeit erneut geprüft

werden. Diese Wiedervorlagefrist wird ausgehend von dem letzten materiellen Erkenntnisdatum zur Person berechnet und beträgt in der Regel höchstens die Hälfte der zulässigen Speicherfrist.

Ich habe deshalb sowohl die Festsetzung der Wiedervorlagetermine, als auch die Durchführung der Erforderlichkeitsprüfung kontrolliert. Eine unzutreffende Festsetzung des Wiedervorlagetermins habe ich dabei nur bei sehr wenigen Speicherungen festgestellt. Nahezu ein Drittel der geprüften Speicherungen war nach Wiedervorlage gelöscht worden, was den Schluss rechtfertigt, dass die notwendige Erforderlichkeitsprüfung vom Landesamt durchgeführt wird. Bei wenigen Speicherungen habe ich das Landesamt wegen fehlenden Aktenrückhalts zur Löschung aufgefordert. Diesen Forderungen ist das Landratsamt ungehend nachgekommen.

8.5 Errichtungsanordnung für das Dokumentenmanagementsystem DOMEA

Seit dem 01.01.2003 darf das Landesamt für Verfassungsschutz nach dem Bayerischen Verfassungsschutzgesetz (Art. 4 Abs. 1 Satz 2, Art. 7 Abs. 1 Satz 3) personenbezogene Daten auch für die Vorgangsverwaltung nutzen und verarbeiten. Im Hinblick darauf wurde mir vom LfV die geplante Änderung der Errichtungsanordnung für das Dokumentenmanagementsystem DOMEA vorgelegt, in dem solche Daten gespeichert werden. Ich habe dem LfV hierzu meine datenschutzrechtlichen Forderungen übermittelt. Diesen hat das LfV weitgehend Rechnung getragen.

8.6 Gemeinsame Datei von Verfassungsschutz und Polizei im Bereich des islamistischen Terrorismus

Besonders seit den Anschlägen des 11. September 2001 wurde der Ruf nach engerer Zusammenarbeit zwischen den Verfassungsschutzbehörden und der Polizei laut. Zwar bestehen schon bisher gesetzliche Grundlagen für eine begrenzte Zusammenarbeit, die insbesondere den gegenseitigen Austausch personenbezogener Daten ermöglichen. Bisher gibt es jedoch keinen Informationsverbund zwischen Polizei und Verfassungsschutz. § 6 Bundesverfassungsschutzgesetz sieht im Gegenteil ausdrücklich vor, dass der Abruf im automatisierten Verfahren aus den gemeinsamen Dateien der Verfassungsschutzbehörden durch andere Stellen nicht zulässig ist. Der Datenaustausch zwischen Verfassungsschutz und Polizei erfolgt deshalb im Wege konventioneller Datenübermittlung.

Besonders im Hinblick auf die Bedrohung durch den internationalen islamistischen Terror wird nunmehr eine gemeinsame Datei zwischen Polizei und Verfassungsschutz gefordert, auf die alle Verbundteilnehmer im Interesse einer zentralen Informationsmöglichkeit zugreifen können. Das Land Niedersachsen hat bereits den Entwurf eines Gesetzes zur Einrichtung einer gemeinsamen Datei der deutschen Sicherheitsbehörden zur Beobachtung und Bekämpfung des islamistischen Extremismus und Terrorismus vorgelegt.

Ich halte diese Forderung im Grundsatz für gerechtfertigt und habe diese Problematik u.a. auf der diesjährigen Frühjahrskonferenz der Datenschutzbeauftragten des Bundes und der Länder zur Sprache gebracht. Meiner Auffassung nach verstößt ein sachlich begrenzter gemeinsamer Informationsbestand von Polizei und Verfassungsschutz grundsätzlich nicht gegen das sog. Trennungsgebot aus dem Jahre 1949, wonach der Verfassungsschutz keine polizeilichen Befugnisse erhalten soll. Bei Einhaltung entsprechender Rahmenbedingungen (s.u.) erhält er solche Befugnisse nicht. Notwendig sind bereichsspezifische, präzise und normenklare gesetzliche Regelungen, die auch im Hinblick auf das Prinzip der informationellen Gewaltenteilung die Möglichkeiten und Grenzen einer gemeinsamen Datei festlegen. Dabei sind insbesondere folgende restriktiven Vorgaben für eine gezielte projektbezogene Zusammenarbeit einzuhalten:

- Keine allgemeine gemeinsame Datei aller Informationsbestände von Polizei und Verfassungsschutz
- Keine unterschiedslose Zusammenlegung sämtlicher Informationsbestände von Polizei und Verfassungsschutz. Es dürfen nur die Informationen in die Datei aufgenommen werden, die zur Bekämpfung des islamistischen Terrorismus erforderlich sind und die bereits im Rahmen des geltenden Rechts erhoben und übermittelt werden könnten.
- Strikte Zweckbindung der Daten für die Bekämpfung des Terrorismus
- Lückenlose Protokollierung des Abrufs von Daten
- Ausreichende Auskunftsregelung
- Gewährleistung einer effektiven Kontrolle durch die zuständigen Datenschutzbeauftragten

- Zeitliche Begrenzung der gemeinsamen Datei (z.B. auf 2 Jahre)

Der niedersächsische Entwurf erfüllt diese Voraussetzungen insbesondere deshalb nicht, weil er nicht auf den islamistischen Terrorismus beschränkt ist, sondern den Bereich des islamistischen Extremismus mit einbezieht. Mit „Extremismus“ würde ein Gefahrenbereich mit einbezogen, für dessen Bekämpfung/Beobachtung nicht alle an der gemeinsamen Datei beteiligten Sicherheitsbehörden zuständig sind. Dafür ist - soweit ohne polizeirelevantes Verhalten - ausschließlich der Verfassungsschutz zuständig. Die Polizei hat insoweit keine Befugnis, Daten zu erheben.

9 Justiz

Im Berichtszeitraum habe ich anlassunabhängig drei Staatsanwaltschaften vor Ort datenschutzrechtlich geprüft und bei weiteren drei Staatsanwaltschaften die abgeschlossenen Strafverfahren einer Prüfung unterzogen, bei denen in dem Zeitraum 1998 bis 2001 Maßnahmen der akustischen Wohnraumüberwachung gemäß § 100 c Abs. 1 Nr. 3 StPO durchgeführt wurden (s.u. unter 9.3.4). Ferner habe ich bei einer Kommune in ihrer Funktion als Ordnungswidrigkeitenbehörde und einer Justizvollzugsanstalt datenschutzrechtliche Prüfungen durchgeführt.

Neben diesen anlassunabhängigen Prüfungen habe ich anlassbezogene Prüfungen aufgrund von Bürgereingaben durchgeführt und bei Entwürfen von Gesetzen und Verwaltungsvorschriften sowie im Rahmen der Einführung von EDV-Systemen auf Berücksichtigung der datenschutzrechtlichen Erfordernisse hingewirkt.

9.1 Gesetzgebung

9.1.1 Justizkommunikationsgesetz

Die Bundesregierung hat den Entwurf eines **Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz - JKomG)** in den Bundesrat eingebracht. Dieses Gesetz soll für sämtliche Gerichtsbarkeiten mit Ausnahme der Strafgerichtsbarkeit Rechtsgrundlagen für die Führung elektronischer Gerichtsakten und die Übermittlung elektronischer Dokumente zwischen Gerichten und Verfahrensbeteiligten schaffen. Für den Bereich des Strafverfahrens ist lediglich die Möglichkeit der Einreichung elektronischer Dokumente, nicht jedoch eine elektronische Aktenführung vorgesehen. Bestandteil des Gesetzentwurfes ist ferner - einem seit langem geltend gemachten Anliegen der Datenschutzbeauftragten entsprechend (s. 20. Tätigkeitsbericht Nr. 8.1.3.1) - der Entwurf eines **Gesetzes zur Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden nach Beendigung des Verfahrens (Justizaktenaufbewahrungsgesetz - JustAG)**.

Parallel zur Schaffung der rechtlichen Grundlagen des elektronischen Rechtsverkehrs im Justizkommunikationsgesetz werden zur Regelung der erforderlichen organisatorisch-technischen Rahmenbedingungen länderübergreifend sog. organisatorisch-technische Leitlinien geschaffen. Beim Bundesgerichtshof, dem Bundespatentgericht und dem Finanzgericht Hamburg wird der elektronische Rechtsverkehr bereits in Pilotprojekten erprobt.

Gegenüber dem Staatsministerium der Justiz habe ich auf mehrere **datenschutzrechtliche Mängel des vorliegenden Gesetzentwurfes** hingewiesen:

So enthält der Entwurf keine Verpflichtungen der beteiligten Stellen zur verschlüsselten Datenspeicherung. Ferner wird die Auftragsdatenverarbeitung nicht auf besonders vertrauenswürdige Stellen beschränkt. Des Weiteren habe ich im Zusammenhang mit der Übermittlung von elektronischen Akten und Sachverständigengutachten einen einheitlichen Schutzstandard durch Verschlüsselungen und qualifizierte elektronische Signaturen gefordert. Die Vorschriften, die Veröffentlichungen der Gerichte im elektronischen Bundesanzeiger oder auf eigenen Homepages ermöglichen, sollten um Regelungen über Löschungsfristen, den Schutz vor Manipulationen und die Anfertigung von Kopien (z.B. entsprechend der Regelung des § 9 Abs. 2 Sätze 2, 3 Insolvenzordnung) ergänzt werden.

Bezüglich der Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden nach Beendigung des Verfahrens habe ich differenzierte Regelungen für die Aufbewahrung einzelner Aktenbestandteile je nach deren Bedeutung gefordert. So ist z.B. die Aufbewahrung von Urteilen über einen längeren Zeitraum erforderlich als die Aufbewahrung der restlichen Akte. Auch habe ich mich für eine Möglichkeit eingesetzt, sensible Aktenbestandteile, die z.B. aus Dokumentationsgründen nicht vernichtet werden können, zu sperren, und für eine Verpflichtung der aufbewahrenden Stelle, auf Antrag des Betroffenen die Vernichtung von Akten bzw. Aktenteilen zu prüfen. Die Dauer der Aufbewahrungsfristen selbst soll in Rechtsverordnungen festgelegt werden. Ich werde mich dafür einsetzen, dass die Fristen so kurz wie möglich bemessen und anlassbezogen überprüft werden.

9.1.2 Erstes Justizmodernisierungsgesetz

Zu Zwecken der Vereinfachung und Beschleunigung von Verfahrensgängen in der Justiz sind ursprünglich drei Gesetzentwürfe vorgelegt worden: der von der Bundesregierung stammende Entwurf eines **Gesetzes zur Modernisierung der Justiz (Justizmodernisierungsgesetz - JuMoG)**, der von der CDU/CSU-Fraktion stammende Entwurf eines **Ersten Gesetzes zur Beschleunigung von Verfahren der Justiz (1. Justizbeschleunigungsgesetz)** und der von mehreren Ländern - darunter auch Bayern - vorgelegte Entwurf eines **Gesetzes zur Beschleunigung von Verfahren der Justiz (Justizbeschleunigungsgesetz)**.

Zum bayerischen Entwurf habe ich gegenüber dem Staatsministerium der Justiz Stellung genommen. Ich habe die beabsichtigte grundsätzliche Bindungswirkung rechtskräftiger Strafurteile für Zivilverfahren, die denselben Sachverhalt betreffen, kritisiert.

Der Bundestag hat zwischenzeitlich einen auf den verschiedenen Gesetzentwürfen beruhenden Kompromissentwurf eines **„Ersten Gesetzes zur Modernisierung der Justiz - 1. Justizmodernisierungsgesetz“** angenommen, den der Rechtsausschuss des Dt. Bundestages vorgeschlagen hatte. Darin ist die o.g. Bindungswirkung rechtskräftiger Strafurteile nicht mehr enthalten.

Das 1. Justizmodernisierungsgesetz enthält ferner auch eine Änderung des § 38 Zwangsversteigerungsgesetz (vgl. dazu unter 9.2.4).

9.1.3 Erweiterung des Anwendungsbereichs der DNA-Analyse zu Strafverfolgungszwecken

Innerhalb des Berichtszeitraums wurden mehrere Gesetzentwürfe mit dem Ziel einer Erweiterung des Anwendungsbereichs der DNA-Analyse zu Strafverfolgungszwecken eingebracht:

- **Bayern** hat im Bundesrat 2002 den **Entwurf eines Gesetzes zum Schutz der Bevölkerung vor schweren Straftaten** eingebracht. Dieser Entwurf sah u.a. eine Erweiterung des (Straftaten von erheblicher Bedeutung umfassenden) Anlasstatenkataloges für DNA-Analysen auf sämtliche Vergehen mit sexuellem Hintergrund vor. Damit hätten derartige Maßnahmen z.B. auch im Falle sexuell motivierter Beleidigungen durchgeführt werden können. Ferner sah der Entwurf vor, dass in sämtlichen Fällen, in denen Betroffene rechtskräftig wegen einer Vorsatztat zu einer Freiheitsstrafe oder Jugendstrafe ohne Strafaussetzung zur Bewährung verurteilt worden sind, DNA-Maßnahmen angeordnet werden können. Dies würde den Anwendungsbereich im Ergebnis - jedenfalls bei Wiederholungstätern - auf Bagatelltaten wie Leistungserschleichung oder Ladendiebstahl erweitern. Der Bundesrat hat 2003 die Einbringung des Gesetzentwurfes in den Bundestag abgelehnt.

- Im Bundestag wurde 2003 der von der Fraktion der CDU/CSU stammende **Entwurf eines Gesetzes zur Verbesserung des Schutzes der Bevölkerung vor Sexualverbrechen und anderen schweren Straftaten**, der die gleichen Erweiterungen vorsah, abgelehnt.

- Der vom Bundesrat stammende **Entwurf eines Gesetzes zur Erweiterung des Einsatzes der DNA-Analyse bei Straftaten mit sexuellem Hintergrund**, der ebenfalls eine Erweiterung des Anlasstatenkataloges auf Vergehen mit sexuellem Hintergrund vorsah, wurde im Bundestag 2003 in die Ausschüsse verwiesen.

Der Bundestag hat 2003 das auf einem Entwurf der Fraktionen der SPD und des Bündnisses 90/ Die Grünen beruhende **Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften** beschlossen. Daraus ergeben sich insbesondere folgende Änderungen für die DNA-Analyse:

- Gesetzlich erlaubt ist nunmehr auch die - bereits in der Vergangenheit praktizierte - Feststellung des Geschlechts des Spurenverursachers.

- Der Anlasstatenkatalog des § 81 g Abs. 1 StPO wurde um die Straftaten gegen die sexuelle Selbstbestimmung erweitert. Er umfasst damit nunmehr sämtliche im Dreizehnten Abschnitt des StGB enthaltenen Tatbestände (z.B. auch die nach § 183 StGB strafbaren exhibitionistischen Handlungen). Bei diesen Straftaten muss es sich nicht um Straftaten von erheblicher Bedeutung handeln. Erforderlich ist jedoch weiterhin die Prognose zukünftiger Straftaten von erheblicher Bedeutung. Straftaten mit sexuellem Hintergrund kommen hingegen auch künftig nur als Anlasstaten in Betracht, wenn es sich im konkreten Fall um eine Straftat von erheblicher Bedeutung handelt.

Nur einen Tag nach der Annahme dieses Gesetzes und der gleichzeitigen Ablehnung des Gesetzentwurfs zur Verbesserung des Schutzes der Bevölkerung vor Sexualverbrechen und anderen schweren Straftaten haben **Bayern und Hessen** im Bundesrat (einen weiteren) **Entwurf eines Gesetzes zur Verbesserung der Regelungen zur DNA-Analyse** eingebracht. Dieser Gesetzentwurf ist weitgehend identisch mit dem letzten von Bayern eingebrachten, bereits im Bundesrat abgelehnten, Entwurf eines Gesetzes zum Schutz der Bevölkerung vor schweren Straftaten (siehe oben). Zum Teil geht er jedoch noch darüber hinaus. So soll nunmehr die Durchführung von DNA-Maßnahmen auch bei bestimmten Verstößen gegen das Betäubungsmittelgesetz (z.B. unerlaubter Erwerb oder Besitz von Betäubungsmitteln) möglich sein, ohne dass es sich dabei um eine Straftat von erheblicher Bedeutung zu handeln braucht.

Zu diesem Gesetzentwurf habe ich gegenüber den Staatsministerien des Innern und der Justiz Stellung genommen. Darin habe ich u.a. ausgeführt, dass die vorgesehene Gesetzesänderung eine Erweiterung des Anlasstatenkataloges auch auf geringfügige Delikte zur Folge hätte, bei denen in einzelnen Ländern Deutschlands sogar Verfahrenseinstellungen wegen Geringfügigkeit erfolgen würden. Dies halte ich im Hinblick auf die Schwere des mit einer DNA-Analyse verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung für unverhältnismäßig. Es entspricht auch nicht der Rechtsprechung des Bundesverfassungsgerichts.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vom 16.07.2003 (Anlage 8) darauf hingewiesen, dass die Durchführung einer DNA-Analyse im Hinblick auf die derzeit bereits bestehenden und zukünftig in noch weitergehendem Umfang zu erwartenden Erkenntnismöglichkeiten nicht mit der herkömmlichen Maßnahme der erkennungsdienstlichen Behandlung - insbesondere der Abnahme eines Fingerabdrucks - gleichgestellt werden kann. Sie haben sich zwar nicht generell gegen eine Ausweitung des Anwendungsbereichs der DNA-Analyse zu Zwecken der Strafverfolgung ausgesprochen, sich aber insbesondere gegen den Verzicht auf das gesetzliche Erfordernis der Prognose erheblicher zukünftiger Straftaten des Betroffenen und gegen die Übertragung der - aus gutem Grund dem Richter vorbehaltenen - Anordnung derartiger Maßnahmen auf die Polizei gewandt.

9.1.4 Gesetz zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften

Der Freistaat Bayern hatte im Bundesrat den Entwurf eines **Gesetzes zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften** vorgelegt, der u.a. umfangreichere Online-Zugriffe der Staatsanwaltschaften auf polizeiliche Dateien ermöglichen und die Voraussetzungen für Online-Zugriffe der Polizei und der Strafgerichte auf das Zentrale staatsanwaltschaftliche Verfahrensregister schaffen sollte:

- Die Staatsanwaltschaften sollten die Befugnis erhalten, für Zwecke der Strafrechtspflege im automatisierten Verfahren aus den Dateien des Bundeskriminalamts Fahndungsausschreibungen, Daten über Freiheitsentziehungen und über veranlasste DNA-Analysen abzurufen. Darüber hinaus enthielt der Gesetzentwurf eine Ermächtigung, im Wege der Rechtsverordnung weitere im polizeilichen Informationssystem gespeicherte Daten zum automatisierten Abruf der Staatsanwaltschaften freizugeben.

  Gegenüber dem Staatsministerium der Justiz habe ich u.a. gefordert, auf diese Ermächtigung zu verzichten. Die Schaffung einer derartigen Erweiterungsmöglichkeit halte ich für problematisch, weil in polizeilichen Dateien auch Daten gespeichert sind, die im Zusammenhang mit der polizeilichen Gefahrenabwehr erhoben wurden und die den präventiven Aufgaben der Polizei dienen. Für diese Aufgaben besteht aber keine Zuständigkeit der Staatsanwaltschaft. Meine Bedenken wurden jedoch nicht berücksichtigt.

- Gegenstand des Gesetzentwurfs war ferner der Auskunftsanspruch Betroffener aus Verfahrensdateien einzelner Staatsanwaltschaften und dem Zentralen staatsanwaltschaftlichen Verfahrensregister (ZStV). Die mit der Auskunft über noch nicht abgeschlossene oder dem Betroffenen noch nicht bekannt gegebene Ermittlungsverfahren zusammenhängende Problematik habe ich in meinem 20. Tätigkeitsbericht (Nr. 8.2.1.3) und unter Nr. 5.21 dieses Tätigkeitsberichts dargestellt. Eine Statistik des Bundeszentralregisters hat bislang keine konkreten Anhaltspunkte für die befürchtete Ausforschungsgefahr ergeben. Trotzdem haben Staatsanwaltschaften teilweise Verfahren - insbesondere aus dem Bereich der Organisierten Kriminalität - dem ZStV zur Vermeidung einer Ausforschung nicht mehr mitgeteilt.

  Der Entwurf der Neufassung des § 491 StPO sah deshalb ursprünglich vor, dass Betroffenen über die bei der Staatsanwaltschaft anhängigen Verfahren keine Auskunft erteilt wird,

soweit sich das Auskunftsersuchen auf etwaige bei der Staatsanwaltschaft noch nicht erledigte Verfahren bezieht oder überwiegende schutzwürdige Interessen entgegenstehen. Dagegen hatte ich eingewandt, dass allgemeine Bedenken nicht dazu führen können, den derzeit unter bestimmten Voraussetzungen bestehenden Auskunftsanspruch in sämtlichen Fällen aufzuheben. Die endgültige Fassung sieht nunmehr vor, dass Auskünfte über staatsanwaltschaftliche Ermittlungsverfahren innerhalb der ersten sechs Monate nicht erteilt werden. Diese Frist kann unter bestimmten Voraussetzungen verlängert werden.

Zwar stellt diese Regelung im Vergleich zur ursprünglich vorgesehenen Fassung eine Verbesserung dar, sie lässt aber leider eine individuelle Prüfung des Auskunftsantrags nicht zu und reduziert damit den Auskunftsanspruch erheblich.

- Ferner sah der Gesetzentwurf in seiner ursprünglichen Fassung vor, den automatisierten Abruf von Daten aus dem ZStV, der derzeit nach § 493 StPO nur Staatsanwaltschaften möglich ist, auf Strafgerichte und Polizeidienststellen auszuweiten. Voraussetzung für einen Abruf durch Polizeidienststellen sollte sein, dass diese nicht zu Zwecken der Gefahrenabwehr, sondern zu Zwecken der Strafverfolgung tätig werden.

  Um möglichst sicherzustellen, dass Übermittlungen an die Polizei tatsächlich nur erfolgen, soweit diese strafverfolgend tätig ist, habe ich eine umfassende Protokollierung der Abrufe gefordert. Dem ist der Gesetzgeber leider nicht nachgekommen. Gestrichen wurde lediglich die zunächst beabsichtigte Erweiterung der Zugriffsmöglichkeit auf Strafgerichte.

- Schließlich sah der ursprüngliche Gesetzentwurf eine Berechtigung der Staatsanwaltschaften zum automatisierten Abruf von Daten des Zollfahndungsinformationssystems vor. Ich habe insoweit die fehlende Bestimmtheit der Regelung kritisiert. Die Regelung wurde insgesamt aus der endgültigen Gesetzesfassung gestrichen.

Der Bundestag hat zwischenzeitlich das Gesetz in seiner geänderten Fassung angenommen.

9.2 Gerichtlicher Bereich

9.2.1 Geschäftsanweisung für die Geschäftsstellen der Gerichte in Zivilsachen

Das Staatsministerium der Justiz hat die **Geschäftsanweisung für die Geschäftsstellen der Gerichte in Zivilsachen (GAZI; früher GAnwZ)** neu gefasst. Im Rahmen der Neufassung wurde auf meine Anregung hin die den Inhalt von Anträgen auf Bewilligung von Prozesskostenhilfe betreffende Regelung dahin gehend geändert, dass im Rahmen von Bewilligungsanträgen für Verfahren auf Scheidung oder Aufhebung einer Ehe nur noch die Zahl der lebenden Kinder des Antragstellers aufzunehmen ist. Nicht mehr anzugeben sind - im Gegensatz zur früheren Fassung - bereits verstorbene Kinder.

Ferner hatte ich kritisiert, dass der Entwurf der Neufassung eine Änderung der GAZI dahin gehend vorsah, dass von sämtlichen gerichtlichen Schriftstücken, die Gefangenen oder Untergebrachten in Justizvollzugsanstalten zugestellt werden, ein Abdruck für die Akten der Anstalt beizufügen ist. Auf meine Kritik hin hat das Staatsministerium der Justiz die bisherige Regelung beibehalten, nach der ein Abdruck des Schriftstückes für die Anstalt nur dann beizufügen ist, wenn dies nach der Entscheidung des Richters bzw. Rechtspflegers aus fürsorgerischen oder anderen vollzuglichen Gründen angezeigt erscheint.

9.2.2 Zustellung im Zivilverfahren

Ein Betroffener hatte sich an mich gewandt und mir mitgeteilt, dass ihm im Rahmen eines Zivilverfahrens ein Schriftsatz der Gegenseite ohne Umverpackung zugestellt worden war.

Eine derartige offene Zustellung verstößt gegen § 176 Abs. 1 ZPO. Wird der Post im Rahmen eines Zivilverfahrens ein Zustellungsauftrag erteilt, hat die Geschäftsstelle des Zivilgerichts das zuzustellende Schriftstück nach dieser Vorschrift in einem verschlossenen Umschlag zu übergeben.

Ich habe den zuständigen Gerichtspräsidenten gebeten, darauf hinzuwirken, dass in Zukunft zuzustellende Schriftstücke der Post ordnungsgemäß in verschlossenen Umschlägen übergeben werden.

9.2.3 Online-Abrufverfahren für das automatisierte Grundbuch

In meinem 19. Tätigkeitsbericht (Nr. 7.3.4) hatte ich die Entwicklung des maschinell geführten Grundbu-

ches und des damit verbundenen automatisierten Abrufverfahrens dargestellt. Zwischenzeitlich gehören dem Entwicklungsverbund für das zur maschinellen Grundbuchführung genutzte Verfahren SolumSTAR 13 deutsche Länder an. Durch den Kontakt mit Kollegen bin ich auf folgende Probleme gestoßen, die die Abrufmöglichkeiten der Gemeinden betreffen:

- Derzeit wird den am Verfahren SolumSTAR teilnehmenden Gemeinden regelmäßig nur eine Benutzerkennung zugeteilt. Ich halte es jedoch für eine effektive Kontrolle der Abrufe für erforderlich, dass jedem berechtigten Mitarbeiter der Gemeinde eine gesonderte Benutzerkennung zugeteilt wird, so dass sich aufgrund der Protokollierung der Abrufe feststellen lässt, welche Person den einzelnen Abruf vorgenommen hat.

- Zu Kontrollzwecken muss durch den Abrufenden jeweils ein Akten- bzw. Geschäftszeichen eingegeben werden. Die Eingabemaske zeigt jedoch automatisch das Akten- bzw. Geschäftszeichen des letzten Abrufs an. Um auszuschließen, dass diese Daten zur Begründung einer Folgeabfrage einfach übernommen werden, sollte diese Anzeige entfallen.

- Die bestehende landesweite Abrufmöglichkeit der Gemeinden halte ich (zumal vor dem Hintergrund der geplanten Erweiterung auf bundesweite Abfragemöglichkeiten) nicht für erforderlich.

  Zwar können Gemeinden grundsätzlich auch in Bezug auf Grundstücke in anderen Gemeindegebieten ein berechtigtes Interesse an der Einsicht des Grundbuchs bzw. der Erteilung von Abschriften im Sinne der §§ 12, 12 a Grundbuchordnung besitzen. Dies kann z.B. der Fall sein, wenn bei Grundstücken an der Gemeindegrenze eine Klärung von Rechten erforderlich ist, die mit den Nachbargrundstücken zusammenhängen, oder wenn für mehrere Grundstücke im Wege des sog. Personalfolio ein gemeinschaftliches Grundbuchblatt geführt wird, was nach § 4 Abs. 2 Grundbuchordnung auch möglich ist, wenn die Grundbücher von verschiedenen Grundbuchämtern geführt werden. Allerdings werden derartige Fälle regelmäßig Grundstücke betreffen, die im Gebiet von Nachbargemeinden liegen.

  Für angemessen halte ich daher allenfalls ein Verfahren, das Zugriffe der Gemeinden auf die Grundbücher der angrenzenden Gemeinden ermöglicht. Eine darüber hinausgehende Grundbucheinsicht oder Erteilung von Abschriften oder Auskünften sollte in herkömmlicher Weise beantragt werden.

Für Ende des Jahres 2004 ist der Pilotierungsbeginn des künftigen Verfahrens SolumWeb vorgesehen. Wie mir die Präsidentin des Oberlandesgerichts München, unter deren Verantwortung das Verfahren entwickelt und erprobt wird, zugesagt hat, werden bei diesem Verfahren beim Aufruf von Folgemasken die Eingabefelder immer in den ursprünglichen leeren Zustand versetzt werden. Hinsichtlich der übrigen Punkte werde ich beim Staatsministerium der Justiz und bei der Präsidentin des Oberlandesgerichts München auf eine Berücksichtigung datenschutzkonformer Lösungen im Rahmen der zukünftigen Fortentwicklung des Verfahrens hinwirken.

9.2.4 Internet-Veröffentlichung von Zwangsversteigerungsterminen

Mehrere bayerische Amtsgerichte veröffentlichen auf gerichtseigenen Homepages Daten der Zwangsversteigerungstermine in ihrem Zuständigkeitsbereich. Bei zwei Amtsgerichten habe ich festgestellt, dass sie dabei auch den Namen des jeweiligen Eigentümers der von der Zwangsvollstreckung betroffenen Immobilie angegeben haben.

Nach § 38 Zwangsversteigerungsgesetz stand eine derartige Benennung des Schuldners bislang im Ermessen des Gerichts. Für die Entscheidung über eine solche Veröffentlichung waren einerseits die mögliche Steigerung des Bieterinteresses durch eine bestmögliche Identifizierung des Grundstückes, andererseits das Recht des Betroffenen auf informationelle Selbstbestimmung zu berücksichtigen. Insbesondere im Hinblick auf die Möglichkeit des weltweiten Abrufs einer Veröffentlichung im Internet habe ich beide Amtsgerichte um Prüfung gebeten, ob sie - entsprechend der Handhabung der übrigen bayerischen Amtsgerichte - auf die Nennung des Namens des Eigentümers im Rahmen derartiger Veröffentlichungen verzichten können. Beide Amtsgerichte haben sich daraufhin entschlossen, die Namen der Eigentümer künftig im Internet nicht mehr zu veröffentlichen.

Durch das 1. Justizmodernisierungsgesetz (vgl. Nr. 9.1.2) wurde die Regelung des § 38 Zwangsversteigerungsgesetz zwischenzeitlich dahin gehend geändert, dass eine Angabe des Namens des Grundstückseigentümers im Rahmen der Bestimmung des Termins einer Zwangsversteigerung nicht mehr vorgesehen ist.

9.2.5 Beiziehung der Scheidungsakte einer Justizangestellten zu Zwecken der Personalverwaltung

Eine Justizangestellte im befristeten Arbeitsverhältnis hat sich an mich gewandt, weil die Akte ihres Scheidungsverfahrens, das bei dem Gericht anhängig war, bei dem sie gearbeitet hatte, von dem zuständigen Personalsachbearbeiter beigezogen worden war. Hintergrund dafür war, dass der Sachbearbeiter mit ihr ein Gespräch über ihre Arbeitsleistungen führen wollte. Nachdem der Gerichtspräsident, dem die Anhängigkeit des Scheidungsverfahrens bekannt geworden war, ihn gebeten hatte, damit noch zu warten, um die Justizangestellte nicht einer zusätzlichen Belastung auszusetzen, hatte der Personalsachbearbeiter die Akte des Scheidungsverfahrens auf Wunsch des Gerichtspräsidenten beigezogen, um sich und den Gerichtspräsidenten über den Stand des Verfahrens zu informieren. Anschließend hatte er an die Akte versehentlich einen Zettel mit der Aufschrift „Zivilabteilung“ angebracht. Die Akte war daraufhin in das Postfach der Zivilabteilung gelegt worden, wo die in dieser Abteilung tätige Justizangestellte sie offen und für jedermann einsehbar vorgefunden hatte.

Die Beiziehung und die Kenntnisnahme des Inhalts der Scheidungsakte stellen eine Nutzung personenbezogener Daten dar, die jedoch ohne Rechtsgrundlage erfolgt war. Sie war insbesondere nicht aufgrund der Aufsichtsfunktion des Gerichtspräsidenten zulässig, da das Scheidungsverfahren in keinem Bezug zu seiner Aufsichtsfunktion stand. Die Beiziehung der Akte durfte auch nicht zu dem Zweck erfolgen, die Befindlichkeit der Justizangestellten zu klären oder einen geeigneten Termin für ein Personalgespräch mit ihr festzulegen. Dies gilt umso mehr, als in Scheidungsakten typischerweise sehr sensible Daten über eheliche und familiäre Umstände der Parteien sowie über ihre Vermögensverhältnisse enthalten sind und die Darstellung dieser Umstände häufig von hoher Emotionalität geprägt ist.

Die persönliche Entschuldigung des Gerichtspräsidenten bei der betroffenen Justizangestellten ändert nichts daran, dass die Beiziehung der Scheidungsakte einen erheblichen Verstoß gegen den Datenschutz darstellt. Ich habe sie deshalb förmlich nach Art. 31 Abs. 1 Satz 1 BayDSG beanstandet und gefordert, in zukünftigen Fällen bei der Vorbereitung von Personalgesprächen von der Beiziehung solcher Akten abzusehen.

Ferner habe ich dem Gericht mitgeteilt, dass ich es im Hinblick auf die besondere Sensibilität des Inhalts von Scheidungsakten für erforderlich halte, dass diese außerhalb des normalen Geschäftsganges verschlossen weitergeleitet werden, wenn Gerichtsbedienstete Beteiligte des jeweiligen Verfahrens sind.

9.3 Strafverfolgung

9.3.1 Forschungsgeheimnis

Die Problematik des Schutzes personenbezogener Daten, die im Rahmen von Forschungsvorhaben verarbeitet werden, hatte ich zuletzt in meinem 18. Tätigkeitsbericht (Nr. 2.3.2) dargestellt. Problematisch ist insbesondere, dass medizinische Daten, die nach ihrer Erhebung durch Ärzte oder Angehörige anderer Heilberufe strafrechtlich vor Offenbarung und Beschlagnahme geschützt werden, diesen Schutz mit der Übermittlung an Forscher verlieren.

Die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung (Anlage 13) den Bundesgesetzgeber aufgefordert,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten aufzunehmen.

Diese Vorschläge stellen aus der Sicht der Datenschutzbeauftragten einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung dar.

Die Bundesministerin der Justiz, die Staatsministerin der Justiz und das Staatsministerium für Wissenschaft, Forschung und Kunst sehen demgegenüber keinen gesetzgeberischen Handlungsbedarf für eine Ergänzung der Strafprozessordnung, allerdings ohne auf das Problem des mangelnden Schutzes von medizinischen Daten in der Forschung im Einzelnen einzugehen. Die Staatsministerin der Justiz hat u.a. darauf hingewiesen, dass Fälle, in denen Forscher gegen die ihnen von den übermittelnden Stellen regelmäßig auferlegte Verschwiegenheitspflicht verstoßen haben, ihrer Kenntnis nach nicht bekannt geworden seien. Das ist aber nur die eine Seite der Problematik. Wesentlich ist, dass ohne ein Forschungsgeheimnis bezüglich der medizinischen Daten weder ein Beschlagnahmeverbot noch ein Zeugnisverweigerungsrecht besteht. Es gibt deshalb eine echte Schutzlücke für medizinische Daten in der Forschung. Vor allem wegen dieses fehlenden strafprozessualen Schutzes der Forscher ist der derzeitige Schutz medizinischer Daten nicht ausreichend. Die Bundesministerin der Justiz hat die Prüfung einer Änderung des Strafge-

setzbuchs zum Schutz des Forschungsgeheimnisses in Aussicht gestellt.

9.3.2 Schutz von Berufsgeheimnisträgern gegen heimliche Überwachungsmaßnahmen

Nach § 53 StPO steht sog. Berufsgeheimnisträgern (z.B. Geistlichen, Rechtsanwälten, Ärzten, Abgeordneten und Journalisten) über Tatsachen, die ihnen im Rahmen ihrer besonders geschützten beruflichen Tätigkeit bekannt geworden sind, ein Zeugnisverweigerungsrecht zu. Der Schutz dieser Berufsgeheimnisträger gegen heimliche Ermittlungsmaßnahmen ist jedoch nur sehr lückenhaft und inkonsequent geregelt. Grundsätzlich sieht die Strafprozessordnung keinen Schutz von Berufsgeheimnisträgern gegen heimliche Überwachungsmaßnahmen vor. Ausnahmen existieren nur hinsichtlich Wohnraumüberwachungsmaßnahmen (§ 100 d Abs. 3 StPO) und - für einzelne Berufsgeheimnisträger (aber z.B. nicht Ärzte oder Journalisten) - hinsichtlich der Einholung von Auskünften über Telekommunikationsverbindungsdaten (§ 100 h Abs. 2 StPO).

Ich halte grundsätzlich einen einheitlichen Schutz von Berufsgeheimnisträgern bei allen verdeckten strafprozessualen Ermittlungsmaßnahmen für angemessen. Dieser könnte in einem einheitlichen Gesamtkonzept geregelt werden. Zum Schutz des Zeugnisverweigerungsrechts der Berufsgeheimnisträger sollte eine Datenerhebung über die mit ihnen geführte Kommunikation soweit möglich nicht stattfinden. Gleichwohl durch heimliche Überwachungsmaßnahmen erlangte Erkenntnisse sollten von einer Verwertung ausgeschlossen sein, sofern nicht der Berufsgeheimnisträger einer Teilnahme oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist.

9.3.3 Wohnungsdurchsuchungen auf Gefahr im Verzug

Wohnungsdurchsuchungen dürfen nach § 105 Abs. 1 StPO grundsätzlich nur durch den Richter als eine unabhängige und neutrale Instanz angeordnet werden. Lediglich bei Gefahr im Verzug ist die Anordnung auch durch die Staatsanwaltschaft oder deren polizeiliche Ermittlungspersonen zulässig. Das Bundesverfassungsgericht hat im Jahr 2001 klargestellt, dass eine solche Eilanordnung der Ausnahmefall sein muss. Es hat zur Wahrung des Grundrechtsschutzes der Betroffenen deshalb gefordert, dass

- die für die Organisation der Gerichte zuständigen Organe in personeller, sachlicher und organisatorischer Hinsicht die erforderlichen Voraussetzungen für eine effektive richterliche Kontrolle sicherstellen,

- die Annahme von Gefahr im Verzug einzelfallbezogen anhand konkreter Tatsachen begründet wird und

- der handelnde Beamte vor oder jedenfalls unmittelbar nach der Durchsuchung die Voraussetzungen der Maßnahme in der Ermittlungsakte dokumentiert, um eine spätere gerichtliche Nachprüfung zu ermöglichen. Insbesondere muss dokumentiert werden, warum ein Aufschieben der Wohnungsdurchsuchung nicht möglich war und ob der Beamte versucht hat, den zuständigen Ermittlungsrichter zu erreichen.

Die praktische Umsetzung der Vorgaben des Bundesverfassungsgerichts habe ich bei einer Staatsanwaltschaft geprüft. Dabei zeigten sich allerdings deutliche Mängel:

- In den meisten Fällen erfolgte die Anordnung nicht durch die Staatsanwaltschaft, sondern durch die Polizei. Dies ist zwar gesetzlich zulässig, führt allerdings dazu, dass eine juristische Kontrolle der Anordnungsvoraussetzungen nicht erfolgt. Aus diesem Grund halte ich es für wünschenswert, dass derartige Maßnahmen grundsätzlich durch die Staatsanwaltschaft angeordnet werden.

- In den Fällen, in denen die Polizei die Wohnungsdurchsuchung auf eine telefonische Anordnung der Staatsanwaltschaft hin durchführte, ließ sich den Ermittlungsakten teilweise nicht entnehmen, welcher Staatsanwalt die Maßnahme angeordnet hatte. Für eine effektive Kontrolle erscheint es mir jedoch erforderlich, dass sich die anordnende Person der Ermittlungsakte entnehmen lässt.

  Die Staatsanwaltschaft hat zwischenzeitlich mitgeteilt, dass nunmehr sämtliche staatsanwaltschaftlichen Durchsuchungsanordnungen mit einem Vordruck dokumentiert werden, der Unterschrift und Namensstempel des anordnenden Staatsanwalts vorsieht. Damit ist gewährleistet, dass sich dessen Identität der Akte entnehmen lässt.

- Die Dokumentation der gesetzlichen Voraussetzungen war häufig nur durch Ankreuzen vorgegebener Formtexte erfolgt. Dies entspricht nicht der vom Bundesverfassungsgericht geforderten Dokumentation einer einzelfallbezogenen und mit konkreten Tatsachen

belegten Prüfung. Teilweise war die auf dem Dokumentationsbogen vorgesehene Begründung sogar gänzlich unterblieben.

Damit die vom Bundesverfassungsgericht aufgestellten Anforderungen in der Praxis umgesetzt werden, habe ich mich vor kurzem an das Staatsministerium der Justiz und das Staatsministerium des Innern gewandt. Eine Antwort steht bislang noch aus.

9.3.4 Akustische Wohnraumüberwachung

In dem Zeitraum von 1998 bis 2001 wurden in Bayern in insgesamt sieben abgeschlossenen Strafverfahren akustische Wohnraumüberwachungen gemäß § 100 c Abs. 1 Nr. 3 StPO durchgeführt. Diese Verfahren habe ich im Hinblick auf mögliche Mängel in der praktischen Umsetzung der rechtlichen Vorgaben einer datenschutzrechtlichen Prüfung unterzogen. Die Frage der Anordnung ist meiner Kontrollkompetenz entzogen, da sie richterlich erfolgt (§ 100 d Abs. 2 StPO, Art. 30 Abs. 4 Satz 2 BayDSG). Mängel waren dabei vor allem in zwei Bereichen festzustellen: Zum einen unterblieb häufig die in § 101 Abs. 1 Satz 1 StPO vorgeschriebene Benachrichtigung der Beteiligten über die durchgeführte Maßnahme. Ferner war in mehreren Fällen die nach §§ 100 d Abs. 4 Satz 3 i.V.m. 100 b Abs. 6 StPO notwendige Vernichtung der durch die Maßnahme erlangten Unterlagen, die zur Strafverfolgung nicht mehr erforderlich waren, unterblieben.

Zur Frage der Benachrichtigung der Betroffenen wurde von den geprüften Staatsanwaltschaften teilweise die Auffassung vertreten, eine ausdrückliche Benachrichtigung sei nicht erforderlich, wenn der Betroffene bzw. sein Verteidiger im Rahmen einer gewährten Akteneinsicht die Möglichkeit hatte, Kenntnis von der durchgeführten Maßnahme zu erlangen. Dies erscheint mir problematisch, da es sich bei der Benachrichtigung um eine Pflicht der Staatsanwaltschaft handelt und die Verantwortung für die Information des Betroffenen nicht ohne weiteres dem Verteidiger übertragen werden kann. Gegenüber dem Staatsministerium der Justiz habe ich ausgeführt, dass ein Verzicht auf eine ausdrückliche Benachrichtigung des Betroffenen im Zusammenhang mit einer gewährten Akteneinsicht allenfalls dann in Frage kommt, wenn der Verteidiger bei der Zuleitung der Akten ausdrücklich auf die durchgeführte Maßnahme hingewiesen wurde.

Die unterbliebene Vernichtung der erlangten Unterlagen war durch die Staatsanwaltschaften in mehreren Fällen damit begründet worden, dass die Unterlagen noch für evtl. Wiederaufnahmeverfahren benötigt würden. Diese Begründung erscheint mir ungeeignet, da ein Wiederaufnahmeverfahren - jedenfalls theoretisch - in keinem Fall ausgeschlossen werden kann, so dass sich im Hinblick darauf eine Aufbewahrung der Unterlagen immer rechtfertigen ließe. Ich habe daher dem Staatsministerium der Justiz mitgeteilt, dass nach meiner Ansicht eine Aufbewahrung der Unterlagen im Hinblick auf etwaige Wiederaufnahmeverfahren nur dann zulässig ist, wenn im konkreten Fall Anhaltspunkte für die Stellung eines Antrags auf Durchführung eines Wiederaufnahmeverfahrens vorliegen.

Zur Sicherstellung datenschutzrechtlicher Belange, insbesondere auch der Einhaltung der Vorgaben des Bundesverfassungsgerichts, hat das Staatsministerium der Justiz - wie schon zuvor für Telekommunikationsüberwachungsmaßnahmen - auf meine Anregung einen **Dokumentationsbogen** für Wohnraumüberwachungsmaßnahmen für die Staatsanwaltschaften entwickelt. Dazu habe ich Änderungsvorschläge gemacht, insbesondere im Hinblick auf eine verbesserte Dokumentation der Umsetzung der gerichtlichen Anordnung und der Gründe für eine Weitergabe der erlangten Unterlagen für andere repressive und präventive Verfahren. Das Staatsministerium der Justiz hat mir mitgeteilt, dass in dem Dokumentationsbogen ein an den Verteidiger im Rahmen der Akteneinsicht zu richtender Hinweis auf die durchgeführte Maßnahme vorgesehen ist.

9.3.5 Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung

Das Bundesverfassungsgericht hat in seinem Urteil vom 03.03.2004 wesentliche Teile der gesetzlichen Regelung der akustischen Wohnraumüberwachung zur Strafverfolgung mit dem Grundgesetz für unvereinbar erklärt. Zum Schutz der Menschenwürde der Betroffenen hat es insbesondere folgende Anforderungen an die Zulässigkeit und Durchführung dieser Maßnahme gestellt:

- Eine Überwachung von Gesprächen mit engsten Familienangehörigen oder Vertrauten sowie bestimmten Berufsgeheimnisträgern ist wegen des damit verbundenen Eingriffs in den Kernbereich privater Lebensgestaltung grundsätzlich nicht zulässig. Stellt sich während der Maßnahme unerwartet heraus, dass die Überwachung diesen Kernbereich berührt, so muss sie abgebrochen werden. Aufzeichnungen derartiger Gespräche dürfen nicht verwertet werden. Die Strafverfolgungsbehörden sind verpflichtet, sie unverzüglich zu löschen.

- Die Anlasstaten, aufgrund derer die Wohnraumüberwachung durchgeführt werden darf,

müssen besonders schwerwiegend sein. Dies bedeutet, dass das Gesetz eine Höchststrafe von mehr als fünf Jahren Freiheitsstrafe vorsehen muss. Zusätzlich muss es sich aber auch im konkreten Einzelfall um eine besonders schwerwiegende Straftat handeln.

- Auch Drittbetroffene sind zu benachrichtigen, sofern nicht die darin liegende Vertiefung des Grundrechtseingriffs bei anderen Betroffenen schwerer wiegt als das Unterlassen der Benachrichtigung gegenüber den Drittbetroffenen. Die Benachrichtigungspflicht kann ferner entfallen, wenn die Feststellung der Identität oder des Aufenthalts des Drittbetroffenen aufwändige Ermittlungen voraussetzt.

- Eine einmalige gerichtliche Kontrolle der Zurückstellung der Benachrichtigung genügt den verfassungsrechtlichen Anforderungen nicht. Vielmehr muss die weitere Zurückstellung regelmäßig gerichtlich kontrolliert werden.

- Personenbezogene Daten dürfen in anderen Verfahren nur zur Aufklärung ähnlich schwerwiegender Straftaten oder zur Abwehr konkreter Gefahren für hochrangige Rechtsgüter verwendet werden.

- Die aus der Maßnahme erlangten Daten sind zur Sicherung der Zweckbindung zu kennzeichnen.

Das Bundesverfassungsgericht hat dem Gesetzgeber zur Schaffung einer gesetzlichen Regelung, die diesen Anforderungen entspricht, eine Frist bis 30.06.2005 gesetzt. Bereits bis zu diesem Termin dürfen die derzeit noch geltenden Vorschriften nur unter Berücksichtigung der o.g. Anforderungen angewandt werden. Darauf habe ich die Staatsministerien der Justiz und des Innern hingewiesen.

Die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung klargestellt, dass die Ausführungen des Bundesverfassungsgerichts auch für die anderen Befugnisse zur verdeckten Datenerhebung im präventiven und repressiven Bereich von Bedeutung sind, und die Gesetzgeber des Bundes und der Länder aufgefordert, zügig die einschlägigen Vorschriften diesen Grundsätzen anzupassen und bei der praktischen Umsetzung der bestehenden Regelungen bereits jetzt die Vorgaben des Gerichts zu beachten (Anlage 18).

Das Bundesministerium der Justiz hatte im Anschluss an die Entscheidung des Bundesverfassungsgerichts zunächst einen - insbesondere im Hinblick auf den Straftatenkatalog und den Schutz von sog. Berufsgeheimnisträgern unzureichenden - Referentenentwurf eines **Gesetzes zur Umsetzung des Urteils des Bundesverfassungsgerichts** vorgelegt. Auf die von den Datenschutzbeauftragten an diesem Entwurf geäußerte Kritik hin liegt zwischenzeitlich ein Gesetzentwurf der Bundesregierung vor, der in zwei Punkten datenschutzrechtliche Verbesserungen gegenüber dem ursprünglichen Entwurf enthält:

- So sollte nach dem ursprünglichen Entwurf der derzeit mit einer Höchststrafe von fünf Jahren bedrohte „besonders schwere Fall der Bildung einer kriminellen Vereinigung“ im Straftatenkatalog enthalten bleiben. Um die vom Bundesverfassungsgericht aufgestellte Bedingung zu erfüllen, wonach Katalogtaten nur besonders schwerwiegende Straftaten sein können, nämlich solche, für die das Gesetz eine Höchststrafe von mehr als fünf Jahren Freiheitsstrafe vorsieht, sah der Gesetzentwurf eine Heraufsetzung der Höchststrafe auf zehn Jahre vor. Dies stellte im Ergebnis eine Umgehung der Anforderungen des Bundesverfassungsgerichts dar.

  Auf die von den Datenschutzbeauftragten erhobene Kritik hin wurde die vorgesehene Heraufsetzung der Höchststrafe aus dem Gesetzentwurf gestrichen. Im aktuellen Entwurf ist der „besonders schwere Fall der Bildung einer kriminellen Vereinigung“ nicht mehr im Katalog enthalten.

- Die zunächst beabsichtigte Regelung der Überwachung sog. Berufsgeheimnisträger stellte eine deutliche datenschutzrechtliche Verschlechterung gegenüber dem derzeitigen Rechtszustand dar. Derzeit sind Wohnraumüberwachungsmaßnahmen gegen diesen zeugnisverweigerungsberechtigten Personenkreis unzulässig. Zukünftig sollten Berufsgeheimnisträger - mit Ausnahme der Verteidiger und Geistlichen, denen (allerdings auch nur, soweit Äußerungen aus dem Mandatsverhältnis bzw. Beichtgespräche oder Gespräche mit beichtähnlichem Charakter betroffen waren) eine Sonderstellung eingeräumt wurde - überwacht werden dürfen, soweit dies im Einzelfall „unabweisbare Bedürfnisse einer wirksamen Strafverfolgung unter besonderer Beachtung des Grundsatzes der Verhältnismäßigkeit“ erforderten. Diese Ausweitung der Überwachungsmöglichkeiten stand in klarem Widerspruch zu der dem Urteil des Bundesverfassungsgerichts zugrunde liegenden Wertung, die Wohnraumüberwachung als

schwerwiegenden Eingriff nur unter ganz engen Voraussetzungen zuzulassen.

Aufgrund der Kritik nicht nur der Datenschutzbeauftragten, sondern besonders auch der betroffenen Berufsverbände sieht der aktuelle Entwurf eine Reduzierung des bestehenden Schutzes der Berufsgeheimnisträger nicht mehr vor.

Auch wenn der neue Entwurf begrüßenswerte datenschutzrechtliche Verbesserungen enthält, entspricht er in einigen Punkten (z.B. hinsichtlich der Fernwirkung von Verwendungsbeschränkungen) noch nicht den datenschutzrechtlichen Forderungen.

Da auch bei anderen verdeckten Ermittlungsmaßnahmen wie der Telekommunikationsüberwachung (§ 100 a StPO) oder dem Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Wortes mit technischen Mitteln außerhalb von Wohnungen (§ 100 c Abs. 1 Nr. 2 StPO) die Vorgaben des Bundesverfassungsgerichts zu beachten sind, besteht noch weiterer gesetzgeberischer Änderungsbedarf. So ist z.B. der Katalog der Anlasstaten für die Telekommunikationsüberwachung nach Jahren der stetigen Erweiterung einer kritischen Überprüfung und ggf. Reduzierung auf ein vertretbares Maß zu unterziehen.

9.3.6 Telekommunikationsüberwachungsmaßnahmen

Die praktische Durchführung von Telekommunikationsüberwachungsmaßnahmen nach § 100 a StPO habe ich bei einer Staatsanwaltschaft überprüft. Die Frage der Anordnung ist gem. Art. 30 Abs. 4 Satz 2 BayDSG meiner Kontrollkompetenz grundsätzlich entzogen, da sie regelmäßig durch den Richter erfolgt (§ 100 b Abs. 1 StPO). Datenschutzrechtliche Mängel waren - entsprechend meinen Feststellungen zur akustischen Wohnraumüberwachung (vgl. oben unter 9.3.4) - vor allem hinsichtlich der Benachrichtigung der Beteiligten über die durchgeführte Maßnahme und hinsichtlich der Vernichtung der erlangten Unterlagen festzustellen.

Einen Verzicht auf eine ausdrückliche Benachrichtigung des Betroffenen im Hinblick auf die ihm oder seinem Verteidiger erteilte Akteneinsicht halte ich nur dann für zulässig, wenn der Betroffene bzw. sein Verteidiger in geeigneter Weise (z.B. durch einen Hinweis auf dem Begleitschreiben, mit dem die Akte zur Akteneinsicht an den Verteidiger übersandt wird) auf die Durchführung der Maßnahme hingewiesen worden sind. Unterbleibt eine Benachrichtigung des von der Maßnahme Betroffenen, halte ich es für erforderlich, die Gründe aktenkundig zu machen.

Bei der Frage, wer zu benachrichtigen ist, ist auch zu berücksichtigen, dass eine Information von Gesprächsteilnehmern einen weiteren Eingriff in das Recht des betroffenen Beschuldigten auf informationelle Selbstbestimmung darstellt, da sie auf diesem Wege Kenntnis davon erhalten, dass gegen den Beschuldigten Abhörmaßnahmen im Rahmen eines Strafverfahrens durchgeführt wurden. Neben dem Beschuldigten und dem Inhaber des überwachten Anschlusses sind jedenfalls Personen, die den Anschluss regelmäßig mitbenutzen (z.B. Familienangehörige oder sonstige Mitbewohner), zu unterrichten. Namentlich bekannte Gesprächsteilnehmer sind in den Fällen über die Maßnahme zu unterrichten, in denen Gespräche Akteninhalt geworden sind. In sonstigen Fällen muss aus den o.g. Gründen eine Abwägung zwischen den Rechten der Betroffenen und den Rechten der Gesprächspartner erfolgen. Soweit Gespräche z.B. rein geschäftlichen Charakter haben, sollte eine Benachrichtigung der Gesprächsteilnehmer grundsätzlich unterbleiben.

Hinsichtlich der Frage der Vernichtung der aus der Maßnahme erlangten Unterlagen gelten die von mir im Hinblick auf Maßnahmen der akustischen Wohnraumüberwachung dargestellten Grundsätze (vgl. oben unter 9.3.4). Die Staatsanwaltschaft muss im Einzelfall prüfen, ob konkrete Anhaltspunkte für einen Antrag auf Durchführung eines Wiederaufnahmeverfahrens vorliegen. Sofern eine weitere Aufbewahrung der Unterlagen erforderlich erscheint, ist dies im Wege eines Aktenvermerks festzuhalten und zu begründen. Die Begründung kann jedoch nicht auf allgemeine Erwägungen gestützt werden. Vielmehr muss einzelfallbezogen dargelegt werden, aus welchen Gründen davon auszugehen ist, dass die Unterlagen zu späteren Zeitpunkten zu Zwecken der Strafverfolgung benötigt werden. Dies gilt insbesondere dann, wenn eine Maßnahme keine verfahrensrelevanten Ergebnisse erbracht hat, die Unterlagen jedoch trotzdem weiter aufbewahrt werden sollen.

Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung waren Gegenstand einer Untersuchung des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg. Das im Auftrag des Bundesministeriums der Justiz erstellte Gutachten des Max-Planck-Instituts hat u.a. festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen Telekommunikationsüberwachungsmaßnahmen angeordnet wurden, sich von 1996 bis 2001 um 80 % erhöht hat,

- die Gesamtzahl der Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 um das Sechsfache gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 fast verdreifacht hat und

- fast Dreiviertel der betroffenen Anschlussinhaber nicht über die Maßnahme unterrichtet wurden.

Die 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung (Anlage 12) den Gesetzgeber und die zuständigen Behörden aufgefordert, aus den Ergebnissen der Untersuchung Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden.

- Der Umfang des Straftatenkataloges des § 100 a StPO muss reduziert werden.

- Um den Schutz der Rechte der Betroffenen sicherzustellen, ist der Kreis der zu benachrichtigenden Personen im Gesetz näher zu definieren. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung vorzusehen.

- Schließlich ist zum Schutz persönlicher Vertrauensverhältnisse eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

Gerade in die entgegengesetzte Richtung zielt jedoch ein vom Freistaat Bayern zusammen mit Hessen im Bundesrat eingebrachter Entwurf vom 23.02.2004 zu einem **„Gesetz zur Verbesserung der Überwachung der Telekommunikation (TKÜ-Verbesserungsgesetz)“**. Dieser Gesetzentwurf sieht u.a. folgende Gesetzesänderungen vor:

- Der Straftatenkatalog des § 100 a StPO soll erweitert werden.

  Dies habe ich gegenüber dem Staatsministerium der Justiz kritisiert. Nachdem das Bundesministerium der Justiz als Konsequenz aus der Entscheidung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 03.03.2004 eine Novellierung der heimlichen Ermittlungsmaßnahmen - insbesondere der Telekommunikationsüberwachung und der akustischen Wohnraumüberwachung - mit dem Ziel einer harmonischen Gesamtregelung angekündigt und das Bundesverfassungsgericht konkrete Vorgaben zur Reduzierung des Straftatenkataloges des § 100 c Abs. 1 Nr. 3 StPO gemacht hat, ist aus meiner Sicht auch der Straftatenkatalog des § 100 a StPO einer kritischen Würdigung mit dem Ziel einer Reduzierung zu unterziehen.

- Durch eine Aufhebung von § 100 h Abs. 2 StPO soll das bislang bestehende Beweiserhebungs- und -verwertungsverbot hinsichtlich einer Auskunftserteilung über Telekommunikationsverbindungen mit Geistlichen, Verteidigern und Abgeordneten entfallen.

  Ich habe mich dagegen ausgesprochen, weil ich diese Änderung für nicht vereinbar halte mit den Grundsätzen des Urteils des Bundesverfassungsgerichts vom 03.03.2004 (vgl. dazu oben unter 9.3.5). Nach den Ausführungen des Bundesverfassungsgerichts besteht insbesondere bei den Zeugnisverweigerungsrechten der Geistlichen und Strafverteidiger ein enger Zusammenhang mit der Menschenwürde des Betroffenen. Eine Kenntnisnahme von den näheren Umständen ihrer Telekommunikationskontakte mit Betroffenen einer Überwachungsmaßnahme ist damit unvereinbar.

- Der bislang auf die Regelung des § 100 i StPO (Maßnahmen bei Mobilfunkendgeräten) gestützte Einsatz des sog. IMSI-Catchers soll in die Regelung des § 100 c Abs. 1 Nr. 1 lit. b StPO (sonstige besondere für Observationszwecke bestimmte technische Mittel) aufgenommen werden.

  Auch hiergegen habe ich mich ausgesprochen, da die Neuregelung die Voraussetzungen für den Einsatz des IMSI-Catchers erheblich herabsetzen würde.

Der Gesetzentwurf befindet sich derzeit in den Ausschüssen des Bundesrates.

9.3.7 Geschäftsstellenautomationsverfahren für Staatsanwaltschaften SIJUS-STRAF-StA

In meinem 20. Tätigkeitsbericht (8.2.5) hatte ich über die Entwicklung der Geschäftsstellenautomation bei den Staatsanwaltschaften berichtet. Das Staatsministerium der Justiz ist derzeit noch mit der Erarbeitung des Entwurfs einer Neufassung der **Dienstanweisung für SIJUS-STRAF-StA** befasst. Es hat mir mitgeteilt, dass beabsichtigt sei, die in der geltenden Dienstanweisung enthaltene Regelung, die eine Datensperre bei Vorgängen gegen Strafunmündige und bei festgestellter Unschuld vorsieht (in Abweichung von der Stellungnahme der Arbeitsgruppe „Daten-

schutzrechtliche Anforderungen an die Geschäftsstellenautomation der Staatsanwaltschaften“ der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz) auch in die Neufassung der Dienstanweisung zu übernehmen.

Nach wie vor umsetzungsbedürftig sind meine Forderungen nach **Sperrung der Daten der Opfer von Sexualdelikten und der Protokollierung von internen Lesezugriffen.** Bezüglich der Protokollierung vertritt das Staatsministerium der Justiz die Auffassung, dass die Regelung des § 488 Abs. 3 Sätze 4, 5 StPO, die lediglich eine Protokollierungspflicht für Lesezugriffe Externer anordnet, eine abschließende Regelung darstelle. Aus meiner Sicht stellt diese Vorschrift jedoch nur einen gesetzlich geregelten Mindestschutz der Betroffenen dar. Ich halte deshalb nach wie vor eine allgemeine Protokollierung von Lesezugriffen (auch innerhalb der jeweiligen Behörde) für geboten.

Das Staatsministerium der Justiz zeigt sich zur weiteren Erörterung dieser offenen Punkte bereit.

9.3.8 Akteneinsicht für Anzeigeerstatter

Eine Bekannte der betroffenen Eingabeführerin hatte gegen sie Strafanzeige wegen Missbrauchs von Titeln erstattet, nachdem die Betroffene unbefugterweise einen akademischen Titel geführt hatte. Die Titelführung war allerdings nicht gegenüber der Anzeigeerstatterin, sondern ausschließlich gegenüber Dritten geschehen. Die Anzeigeerstatterin war somit durch die angezeigte Straftat nicht verletzt.

Der Rechtsanwalt der Anzeigeerstatterin beantragte während des laufenden Ermittlungsverfahrens Akteneinsicht bei der Staatsanwaltschaft. Zur Begründung führte er aus, nachdem Gerüchten zufolge das Ermittlungsverfahren eingestellt worden sei, benötige er die erbetene Akteneinsicht zur Beurteilung des Sachstandes. Die Staatsanwaltschaft gewährte dem Rechtsanwalt die beantragte Akteneinsicht. In der Akte befanden sich auch Informationen über ein früheres Verfahren, in dem die Betroffene freigesprochen worden war, nachdem - nach vorausgegangener Verurteilung - nicht auszuschließen war, dass sie im Zustand der Schuldunfähigkeit gehandelt hatte.

Der Vorgang ist über den Einzelfall hinaus von Bedeutung, da er die Problematik der Akteneinsicht durch einen durch die Straftat nicht verletzten Anzeigeerstatter aufzeigt.

Da die Anzeigeerstatterin nicht Verletzte der angezeigten Straftaten war, konnte die Akteneinsicht nicht auf die - die Erteilung von Akteneinsicht an den Verletzten bzw. dessen Rechtsanwalt regelnde - Vorschrift des § 406 e StPO gestützt werden. Akteneinsicht durfte nach § 475 Abs. 1, 2 StPO nur erteilt werden, soweit ein berechtigtes Interesse dargelegt werden konnte und die Betroffene kein schutzwürdiges Interesse an der Versagung der Akteneinsicht hatte.

Ein berechtigtes Interesse an der Akteneinsicht ergab sich nicht aus etwaigen Unklarheiten über den Stand des Ermittlungsverfahrens. Insoweit wäre eine - gegenüber der Gewährung von Akteneinsicht vorrangige - Auskunft der Staatsanwaltschaft hinreichend gewesen. Auch konnte ein berechtigtes Interesse nicht auf die Möglichkeit des Vertreters der Anzeigeerstatterin gestützt werden, Beschwerde gegen die Einstellungsverfügung einzulegen. Abgesehen davon, dass zu diesem Zeitpunkt die Einstellung des Verfahrens noch gar nicht erfolgt war, stand der Anzeigeerstatterin, da sie nicht Verletzte war, ein formelles Beschwerderecht nach § 172 Abs. 1 StPO gar nicht zu. Allein die Möglichkeit eines nicht verletzten Anzeigeerstatters, gegen eine Einstellung der Staatsanwaltschaft Dienstaufsichtsbeschwerde einzulegen, rechtfertigt regelmäßig nicht die Annahme eines berechtigten Interesses an der Kenntnisnahme des gesamten Akteninhalts.

Gegen die Akteneinsicht sprach das schutzwürdige Interesse der Betroffenen, da sich aus der Akte Informationen über das gegen sie gerichtete frühere Verfahren einschließlich der - 13 Jahre zuvor - erfolgten Verurteilung und der verhängten Strafe sowie das Wiederaufnahmeverfahren und die damit zusammenhängenden Fragen der Schuldfähigkeit entnehmen ließen.

Ich habe den Leiter der Staatsanwaltschaft gebeten, in zukünftigen Fällen, in denen Anzeigeerstatter Akteneinsicht beantragen, zu prüfen, ob diese Verletzte sind und, falls dies nicht der Fall ist, ob sie ein berechtigtes Interesse darlegen und nicht schutzwürdige Interessen des Betroffenen der Gewährung der Akteneinsicht entgegenstehen. Das Ergebnis dieser Prüfung sollte aktenkundig gemacht werden.

Das Staatsministerium der Justiz hat auf meinen Hinweis die Thematik bei einer Dienstbesprechung mit den Leitern der bayerischen Staatsanwaltschaften erörtert. Als Ergebnis der Dienstbesprechung hat mir das Staatsministerium der Justiz Folgendes mitgeteilt:

- Im Einzelfall könne die Prüfung der Einlegung einer Dienstaufsichtsbeschwerde ein berechtigtes Interesse begründen.

- Vorrangig gegenüber der Gewährung von Akteneinsicht sei die Erteilung (partieller) Auskünfte.

- Bei der Prüfung, ob der Betroffene ein schutzwürdiges Interesse an der Versagung habe, seien vor allem Umstände, die den Schutz seiner Privatsphäre berühren, zu berücksichtigen.

- Um dem Spannungsverhältnis zwischen den Interessen der Beteiligten gerecht zu werden, könne es erforderlich sein, Aktenbestandteile, die Rückschlüsse auf die körperliche und geistige Verfassung oder bestehende Vorahndungen des Betroffenen zulassen, vor Erteilung der Akteneinsicht aus der Akte zu entfernen.

Diese Feststellungen erscheinen mir grundsätzlich zutreffend, insbesondere soweit ein berechtigtes Interesse nur in Ausnahmefällen angenommen wird. Probleme werden sich allerdings auch zukünftig eher bei der Abwägung der gegenläufigen Interessen im Einzelfall ergeben, so dass ich die praktische Umsetzung weiter beobachten werde.

9.4 Justizvollzug

9.4.1 Zentrale Vollzugsdatei

Das Staatsministerium der Justiz beabsichtigt, die erforderliche Übermittlung von personenbezogenen Daten der Justizvollzugsanstalten an andere Justizvollzugsanstalten, Justizbehörden und die Polizei im Wege des automatisierten Abrufs bzw. der automatisierten Übertragung zu ermöglichen. Zu diesem Zweck wurde bereits eine Zentrale Vollzugsdatei eingerichtet, in der die Daten der Gefangenen aller bayerischen Justizvollzugsanstalten zusammengeführt werden. Ein Teil dieser Daten soll automatisiert an einen Kopfstellenrechner des Landeskriminalamtes übermittelt und damit in das polizeiinterne Informationssystem (Haftdatei) einbezogen werden. Justizvollzugsanstalten und Justizbehörden sollen die Möglichkeit erhalten, aus der Zentralen Vollzugsdatei anlassbezogen bestimmte Daten abzurufen.

Für den Datenabruf sieht das Konzept ein nach Benutzergruppen differenziertes System von Zugriffsberechtigungen vor. Danach soll den Mitarbeitern der Strafvollzugsabteilung des Staatsministeriums der Justiz - die die Dienstaufsicht über die Anstalten ausüben und z.B. Eingaben, Beschwerden und Gesuche Gefangener bearbeiten - ein uneingeschränkter Zugriff auf alle Daten der Zentralen Vollzugsdatei ermöglicht werden. Je nach ihrer Tätigkeit eingeschränkten Zugriff sollen ferner folgende Benutzergruppen erhalten:

- Strafrichter und Staatsanwälte

- Familienrichter, Strafvollstreckungsrechtspfleger und Bewährungshelfer

- Sonstige berechtigte Personen bei Gerichten und Staatsanwaltschaften (Richter, Rechtspfleger und Serviceeinheiten)

- Leiter der Justizvollzugsanstalten, ihre Vertreter und die Leiter der Vollzugsgeschäftsstellen

Ich habe mich insbesondere im Hinblick auf den Umfang der geplanten Zugriffsberechtigungen gegenüber dem Staatsministerium der Justiz u.a. wie folgt geäußert:

- Nicht erforderlich erscheinen mir die weitreichenden Zugriffsbefugnisse, die für Familienrichter vorgesehen sind. Diese werden nach Mitteilung des Staatsministeriums der Justiz vorerst keinen Zugriff auf die Zentrale Vollzugsdatei erhalten.

- Nicht gerechtfertigt ist auch, dass den Leitern und Abteilungsleitern der Justizvollzugsanstalten sowie den Leitern der Vollzugsgeschäftsstellen Zugriffsmöglichkeiten auch hinsichtlich Daten Gefangener eingeräumt werden sollen, die in anderen Justizvollzugsanstalten untergebracht sind.

  Das Staatsministerium der Justiz hat hierzu geäußert, der Zugriff sei zur Vorbereitung und Durchführung von vollzuglichen Entscheidungen und Maßnahmen, zur vorbeugenden Gefahrenabwehr und zur Aufrechterhaltung von Sicherheit und Ordnung in den Anstalten unerlässlich. Gerade im Hinblick auf die zunehmend zu beobachtende Tendenz einzelner Gefangenengruppen, sich anstaltsübergreifend zu organisieren und abzustimmen, sei es erforderlich, auch bei allgemeinen vollzuglichen Entscheidungen (Abschätzung einer Gefahrenlage, Erkennen von möglichen Subkulturen, Aufdecken von Verflechtungen und Beziehungen unter Gefangenen) Informationen über Gefangene anderer Anstalten einzuholen. Ferner würden die zum Abruf aus der Zentralen Vollzugsdatei berechtigten Personen ausdrücklich auf die gesetzlichen Voraussetzungen für einen Abruf hingewiesen. Dadurch, dass für jeden Abruf zwingend die Eingabe eines Aktenzeichens notwendig sei, sei sichergestellt, dass auch die Angehörigen dieser Benutzergruppe Daten nur aus konkretem Anlass abrufen.

Dies reicht zur Sicherstellung der datenschutzrechtlichen Anforderungen jedoch nicht aus. Die Einrichtung eines automatisierten Abrufverfahrens ist nach Art. 8 Abs. 1 BayDSG nur zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. In die Prüfung der Angemessenheit sind dabei u.a. folgende Gesichtspunkte mit einzubeziehen: Dringlichkeit eines schnellen, unmittelbaren Zugriffs, Vereinfachung von häufigen Datenübermittlungen, Vermeidung von aufwendig manuell zu bearbeitenden Anfragen und Sensibilität der Anfragen. Wesentlich ist der Bedarf der abrufenden Stelle an einem schnellen, unmittelbaren Zugriff auf die Daten. Je häufiger und je kurzfristiger die Daten benötigt werden und je weniger sensibel die Daten sind, desto eher kann von einer Angemessenheit ausgegangen werden.

Ein Abruf von Daten Gefangener, die in anderen Justizvollzugsanstalten inhaftiert sind, wird im Wesentlichen im Falle ihrer Verlegung erforderlich sein. Verlegungen von Gefangenen begründen jedoch weder die Notwendigkeit eines schnellen, unmittelbaren Zugriffs, noch kann die Vereinfachung der Datenübermittlung auf die Häufigkeit derartiger Verlegungen gestützt werden. Insbesondere im Hinblick auf die Sensibilität der abgefragten Daten halte ich daher die Einrichtung eines automatisierten Abrufverfahrens für diese Fälle nicht für angemessen.

- Den Umfang der Daten, die automatisch an den Kopfstellenrechner des Bayerischen Landeskriminalamtes übermittelt werden sollen, halte ich für zu groß. Nach § 13 Abs. 1 Satz 3 BKAG werden dem zuständigen Landeskriminalamt zwar Beginn, Unterbrechung und Beendigung von Freiheitsentziehungen im Zusammenhang mit rechtswidrigen Taten mitgeteilt. Darüber hinaus können Datenübermittlungen an das Landeskriminalamt zulässig sein, wenn sie im konkreten Einzelfall zur Verhinderung oder Verfolgung von Straftaten erforderlich sind. Dies rechtfertigt jedoch keine generelle Übermittlung solcher Gefangenendaten an das Landeskriminalamt auf Vorrat.

Diese sowie weitere noch offene Fragen sollen im Rahmen einer mündlichen Erörterung zwischen Vertretern des Staatsministeriums der Justiz und mir geklärt werden.

9.4.2 Transport von Gefangenenpersonalakten

Ein Strafgefangener hatte sich an mich gewandt, weil im Rahmen seiner Verlegung aus einer Justizvollzugsanstalt in eine andere seine Gefangenenpersonalakten verloren gegangen waren.

Aus den Stellungnahmen der beteiligten Justizvollzugsanstalten ergab sich folgender Sachverhalt: Im Rahmen der Verlegung des Gefangenen waren die Gefangenenpersonalakten mit auf den Transport gegeben worden. Wegen ihres Umfangs waren sie in Abweichung von der üblichen Handhabung nicht in vorgedruckten Versandumschlägen, sondern in einer Schachtel verpackt worden. Diese war mit anderen Gepäckstücken dem Transportführer übergeben und in der Transportliste als „Päckchen“ bezeichnet worden. Ein Hinweis auf der Verpackung auf die Gefangenenpersonalakten war nicht erfolgt. Auch der Transportliste hatten sich keine Hinweise auf den Inhalt des Päckchens entnehmen lassen. Der Empfang des Päckchens war in der zweiten Justizvollzugsanstalt auf der Transportliste quittiert worden. Der Verbleib der Gefangenenpersonalakten in dieser Justizvollzugsanstalt ließ sich aber nicht mehr aufklären.

Nach § 183 Abs. 2 Satz 1 StVollzG sind Akten und Dateien mit personenbezogenen Daten durch die erforderlichen technischen und organisatorischen Maßnahmen gegen unbefugten Zugang und unbefugten Gebrauch zu schützen. Gegen diese Vorschrift hat die Justizvollzugsanstalt, aus der der Gefangene verlegt wurde, verstoßen, indem die Gefangenenpersonalakten während des Transports nicht äußerlich gekennzeichnet waren und sich auch aus der Transportliste kein Hinweis auf den Inhalt des Päckchens ergab.

Nachdem sich nicht mehr aufklären ließ, was mit dem Päckchen in der zweiten Justizvollzugsanstalt geschehen war, war mir die Feststellung eines datenschutzrechtlichen Verstoßes insoweit nicht möglich.

Ich habe daher die Justizvollzugsanstalt, aus der der Gefangene verlegt worden war, aufgefordert, Gefangenenpersonalakten, die auf den Transport gegeben werden, zukünftig äußerlich zu kennzeichnen. Dies kann insbesondere durch den Gebrauch der üblichen Versandumschläge geschehen. In Fällen wie dem vorliegenden, in denen diese Umschläge aufgrund des Umfangs der Akte nicht benutzt werden können, müssen sonstige Behältnisse, in denen die Gefangenenpersonalakten transportiert werden, entsprechend gekennzeichnet sein. Auch sollte ein entsprechender Eintrag in der Transportliste erfolgen, damit sichergestellt ist, dass die Gefangenenpersonalakten in der Justizvollzugsanstalt, in die sie transportiert werden,

als solche erkannt und ordnungsgemäß behandelt werden.

9.5 Ordnungswidrigkeitenverfahren

9.5.1 Fahrerermittlung durch Lichtbildabgleich

Die Zulässigkeitsvoraussetzungen eines Lichtbildabgleichs mit dem Pass- bzw. Personausweisregister zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr hatte ich zuletzt in meinem 18. Tätigkeitsbericht (Nr. 7.6.4) und in meinem 19. Tätigkeitsbericht (Nr. 7.5.1) dargestellt. Danach muss aufgrund der gesetzlichen Regelungen grundsätzlich folgende Reihenfolge bei der Datenerhebung eingehalten werden:

- Versuch der Datenerhebung beim Betroffenen, d.h. bei demjenigen, in dessen Rechte durch einen späteren Lichtbildabgleich eingegriffen würde

- Abgleich des Tatfotos mit dem Lichtbild aus dem Pass- bzw. Personalausweisregister, falls die Daten beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können

- Eingriffsintensivere Ermittlungsmaßnahmen (insbesondere Umfeldermittlungen durch Befragungen von Nachbarn oder Arbeitskollegen des Betroffenen) kommen im Rahmen der Verhältnismäßigkeit allenfalls dann in Betracht, wenn das mildere Mittel des Bildabgleichs nicht zur Täterermittlung geführt hat.

Diese Reihenfolge ist erneut auch dann einzuhalten, wenn sich der Tatverdacht auf eine andere Person verlagert, weil z.B. die Ordnungswidrigkeitenbehörde zwischenzeitlich davon ausgeht, dass nicht der Fahrzeughalter, sondern ein Angehöriger des Halters gefahren ist. Auch in diesem Fall hat einem Lichtbildabgleich grundsätzlich der Versuch der Datenerhebung beim nunmehr Betroffenen vorauszugehen.

Besonderheiten treten bei Verkehrsverstößen mit Firmenfahrzeugen juristischer Personen auf. Gehen die Ermittlungsbehörden bei Verstößen mit Privatfahrzeugen regelmäßig zunächst davon aus, dass der Fahrzeughalter gefahren ist, so ist dies bei solchen Firmenfahrzeugen nicht möglich, da es sich beim Fahrzeughalter ja gerade nicht um eine natürliche Person handelt. Um überhaupt die Person des Fahrzeugführers feststellen zu können, wird daher regelmäßig die Befragung dritter Personen notwendig sein. So wird z.B. der Inhaber bzw. ein Vertreter der jeweiligen Firma als Zeuge zu der Frage, wer das Tatfahrzeug zur betreffenden Zeit geführt hat, befragt werden müssen. In diesem Zusammenhang erscheint es datenschutzrechtlich gerechtfertigt, ihm das Tatlichtbild vorzulegen, wenn nur so eine Feststellung des Fahrzeugführers möglich erscheint.

Im Zusammenhang mit der Frage, wann davon auszugehen ist, dass die erforderlichen Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können, neigt das Staatsministerium des Innern dazu, das Tatbestandsmerkmal des „unverhältnismäßig hohen Aufwands“ aufgrund der Unterbesetzung bzw. Arbeitsüberlastung der Polizei und der Ordnungswidrigkeitenbehörden und des technischen Fortschritts, der das Verfahren des Lichtbildabgleichs wesentlich vereinfacht habe, einer Neubewertung zu unterziehen. In der Tat hat das Oberlandesgericht Stuttgart in einem Beschluss vom 26.08.2002 die dauernde personelle Unterbesetzung der zuständigen Verwaltungsbehörden und der Polizei und ihre Aufgabenüberlastung sowie die kurze Verjährungsfrist von nur drei Monaten zur Auslegung dieses Tatbestandsmerkmals herangezogen.

Aus meiner Sicht ist die Frage der Verhältnismäßigkeit aufgrund eines Vergleichs zwischen dem Aufwand der Behörde für die Datenerhebung beim Betroffenen und der Intensität des Eingriffs in die Rechte des Betroffenen durch einen sofortigen Bildabgleich zu beurteilen. Der Arbeitsbelastung der Ermittlungsbehörde - die noch dazu von Fall zu Fall und Behörde zu Behörde unterschiedlich sein kann - kommt dabei aus meiner Sicht keine entscheidende Rolle zu. Auch technischer Fortschritt darf nicht zu einer Absenkung der Eingriffsschwelle führen, wenn der Aufwand der einzelnen durchzuführenden Maßnahme (z.B. Schreiben an den Betroffenen) gleich hoch bleibt. Problemen, die sich aus der Personalsituation und Arbeitsbelastung der Behörden sowie der kurzen Verjährungsfrist ergeben, kann durch Verringerung des Arbeitsaufwandes bei der Datenerhebung im Rahmen des geltenden Rechts entgegengewirkt werden. So halte ich es z.B. für ausreichend, wenn der Betroffene einmal - ggf. mit kurzer Fristsetzung - angeschrieben wird. Äußert er sich nicht, kann die Ermittlungsbehörde im Rahmen der gesetzlichen Vorschriften einen Lichtbildabgleich durchführen. Erscheint eine persönliche Anhörung oder eine Inaugenscheinnahme des Betroffenen erforderlich, sollte diesem Gelegenheit zur Vorsprache gegeben werden. Dies ist sowohl arbeitsökonomischer als auch für den Betroffenen datenschutzfreundlicher, als wenn er zu Hause oder an seiner Arbeitsstelle aufgesucht wird.

Ein weiteres Problem bei der praktischen Umsetzung des Lichtbildabgleichs konnte ich im Rahmen der Prüfung einer Polizeidirektion feststellen. Nach den

gesetzlichen Vorschriften hat die um die Übermittlung von Lichtbildern ersuchende Behörde den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen aktenkundig zu machen. Letzteres ist jedoch nicht sichergestellt:

Die von der Zentralen Bußgeldstelle an die Polizeidienststelle übermittelte Verkehrsordnungswidrigkeitenanzeige wird durch diese nach Abschluss der Ermittlungen urschriftlich zurückgesandt. Der Zentralen Bußgeldstelle wird lediglich der ermittelte Fahrer bzw. Halter des Fahrzeugs mitgeteilt. Wie die Polizeidienststelle zu dem Ermittlungsergebnis gelangt ist, wird in der Regel nicht in der Akte vermerkt, so dass auch nicht festzustellen ist, ob die gesetzlichen Voraussetzungen eines Lichtbildabgleichs erfüllt waren. Eine Dokumentation des Ermittlungsvorgangs bei der Polizei findet nur in der polizeilichen Vorgangsverwaltung statt, in der die Halter- bzw. Fahrerermittlung als Ermittlungsersuchen mit dem Namen des Betroffenen und dem Kfz-Kennzeichen festgehalten wird. Nicht festgehalten werden dagegen nähere Umstände, z.B. welche Maßnahmen im Detail (z.B. Lichtbildabgleich) getroffen wurden und ggf. bei wem.

Diese Art der Dokumentation ist nicht ausreichend, um die gesetzlichen Anforderungen zu erfüllen, da die Herkunft der Daten für einen etwaigen Bildabgleich nicht festgehalten wird. Ich habe deshalb die Umsetzung der gesetzlich vorgeschriebenen Dokumentationspflichten beim Staatsministerium des Innern eingefordert.

9.5.2 Melderegisterauskunft bezüglich Angehöriger

Ergibt sich im Rahmen eines Verkehrsordnungswidrigkeitenverfahrens, dass der Verkehrsverstoß nicht durch den Halter des Fahrzeugs begangen wurde, stellt sich für die Ordnungswidrigkeitenbehörde erneut die Frage, welche Person das Fahrzeug geführt hat. Da es nahe liegt, dass der Fahrzeugführer ein Angehöriger des Halters ist, schreiben insbesondere kommunale Verkehrsüberwachungsdienste in derartigen Fällen häufig die Meldebehörde am Wohnsitz des Fahrzeughalters mit der Bitte an, die Personalien von Angehörigen des Fahrzeughalters, die als Fahrer in Frage kommen, mitzuteilen. Melderechtlich ist die Mitteilung von Meldedaten durch die Meldebehörde in diesen Fällen wie folgt zu beurteilen:

Die Meldebehörden dürfen nach Art. 31 Abs. 1 Bayerisches Meldegesetz anderen Behörden bestimmte Daten aus dem Melderegister übermitteln, wenn dies zur Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Vorausgesetzt, dass der Fahrzeughalter im Rahmen seiner Anhörung weder die Fahrereigenschaft eingeräumt hat, noch den Fahrer mitgeteilt hat, halte ich daher die Übermittlung der Daten von Angehörigen des Fahrzeughalters grundsätzlich für zulässig. Sie muss jedoch auf die Übermittlung der Daten der Personen beschränkt werden, die tatsächlich als Fahrer in Betracht kommen. Dies bedeutet, dass z.B. Meldedaten von Kindern, bei denen dies aufgrund ihres Alters ersichtlich nicht der Fall ist, nicht übermittelt werden dürfen. Soweit anhand des Tatfotos weitere Personen z.B. aufgrund ihres Alters oder Geschlechts als mögliche Täter ausgeschieden werden können, dürfen ihre Daten ebenfalls nicht übermittelt werden. Schließlich dürfen keine Meldedaten von Personen, hinsichtlich derer aus sonstigen Gründen keine Anhaltspunkte dafür vorliegen, dass sie das Fahrzeug geführt haben, übermittelt werden. Dies können z.B. entferntere Verwandte (zumal wenn sie nicht im selben Ort wohnen wie der Fahrzeughalter) und namensgleiche Personen, die jedoch nicht mit dem Fahrzeughalter verwandt sind, sein.

Soweit aufgrund der o.g. Kriterien eine Eingrenzung des in Betracht kommenden Täterkreises möglich ist, muss diese bereits in dem Auskunftsersuchen gegenüber der Meldebehörde erfolgen, um die Übermittlung nicht erforderlicher Daten zu vermeiden. Dies geschieht in der Praxis häufig dadurch, dass auf dem Formschreiben angekreuzt wird, auf welche Angehörigen (Ehepartner, Sohn, Tochter, Mutter, Vater) sich die Anfrage bezieht. Ein derart eingeschränktes Auskunftsersuchen halte ich grundsätzlich für zulässig.

Allerdings lassen sich über das Melderegister die Angehörigen einer bestimmten Person nur in begrenztem Umfang feststellen. Gespeichert werden nach Art. 3 Abs. 1 Nr. 9, 15 und 16 Bayerisches Meldegesetz gesetzliche Vertreter, Ehegatten, Kinder bis zur Vollendung des 27. Lebensjahres sowie die Eltern von Kindern bis zur Vollendung des 27. Lebensjahres. Anfragen nach Daten sonstiger Angehöriger (z.B. von Geschwistern) können zwar Erfolg haben, wenn den Meldebeamten (insbesondere in kleineren Gemeinden) über die nach Art. 3 Bayerisches Meldegesetz gespeicherten Daten hinaus Familienangehörige des Betroffenen bekannt sind. Dabei handelt es sich jedoch um „Zufallsfunde“.

In diesem Zusammenhang hatte sich ein Betroffener mit folgendem Sachverhalt an mich gewandt: Er hatte als Fahrzeughalter im Ordnungswidrigkeitenverfahren glaubhaft angegeben, das Tatfahrzeug nicht gefahren zu haben und auch keine Angaben zur Person des Fahrers machen zu können, da auf das Fahrzeug mehrere Personen Zugriff hätten. Nachdem die ermittelnde Polizeidienststelle ihn mehrmals nicht hatte erreichen können, war schließlich eine Befragung seiner Nachbarn unter Vorlage des Lichtbildes, auf

dem sein Bruder als Fahrzeugführer zu erkennen war, erfolgt.

Der Betroffene war der Ansicht, die Polizei hätte vor einer Nachbarschaftsbefragung versuchen müssen, die Identität des Fahrzeugführers über eine Anfrage an das Melderegister festzustellen. Das mit der Sache befasste Polizeipräsidium gab in seiner Stellungnahme an, eine derartige Anfrage sei als nicht erfolgversprechend eingeschätzt und deshalb unterlassen worden. Nachdem aus dem Tatfoto ersichtlich war, dass der Fahrer des Tatfahrzeugs männlich und aufgrund seines Alters nicht davon auszugehen war, dass es sich um einen Sohn des Fahrzeughalters handelte, konnte die Polizeidienststelle eine Anfrage an das Melderegister als nicht erfolgversprechend ansehen, so dass die Nachbarschaftsbefragung mangels anderer vorrangiger Ermittlungsmöglichkeiten datenschutzrechtlich zulässig war.

9.5.3 Postzustellungsurkunde im Ordnungswidrigkeitenverfahren

Ein Betroffener hatte sich an mich gewandt, nachdem im Betreff einer Postzustellungsurkunde, mit der ihm ein Bußgeldbescheid zugestellt worden war - für den Zustellungsbeamten erkennbar -, der Tatvorwurf („Parken im Landschaftsschutzgebiet“) sowie die Gesetze, gegen die der Betroffene verstoßen hatte, angegeben waren.

Dies war unzulässig. Ein derart detaillierter Betreff ist nicht erforderlich, um die Postzustellungsurkunde nach ihrem Rücklauf zur Ordnungswidrigkeitenbehörde dem jeweiligen Vorgang zuordnen zu können.

Nachdem ich mich mit der Ordnungswidrigkeitenbehörde in Verbindung gesetzt habe, hat mir diese zugesichert, künftig auf die Nennung des Tatvorwurfs auf Postzustellungsurkunden zu verzichten.

9.5.4 Anfrage an Bank des Betroffenen

Der Geschäftsführer einer GmbH hatte sich mit folgendem Sachverhalt an mich gewandt:

Auf Grund einer Verkehrsordnungswidrigkeit mit einem Kraftfahrzeug der GmbH war ein Ordnungswidrigkeitenverfahren eingeleitet worden, in dessen Rahmen er als Geschäftsführer der GmbH als Zeuge schriftlich befragt und zugleich auf die Möglichkeit hingewiesen worden war, das Verfahren durch eine Zahlung von € 25,-- abschließend zu erledigen.

Der Betroffene hatte die € 25,-- per Online-Überweisung unter Angabe seines Namens und des Fahrzeugkennzeichens auf das vom Polizeipräsidium angegebene Konto überwiesen. Das Polizeipräsidium hatte den Zahlungseingang jedoch nicht zuordnen können, da dort unter dem angegebenen Autokennzeichen zwei Ordnungswidrigkeiten für die GmbH als Halterin zu je € 25,-- erfasst waren. Das Polizeipräsidium hatte darauf hin die Bank des Betroffenen mit einem Formschreiben angeschrieben und sie gebeten, dieses an den Inhaber des angegebenen Kontos (den Betroffenen) weiterzuleiten. Darin wird dieser unter Bezugnahme auf die Ordnungswidrigkeit gebeten, zur ordnungsgemäßen Verbuchung des überwiesenen Betrages das Aktenzeichen, zumindest aber das amtliche Kennzeichen des beanstandeten Fahrzeugs (das er bereits auf dem Überweisungsträger angegeben hatte) mitzuteilen. Die Bank hat das Schreiben an den Betroffenen weitergeleitet.

Das Schreiben des Polizeipräsidiums an die Bank des Betroffenen stellt eine Übermittlung sensibler personenbezogener Daten an eine nicht-öffentliche Stelle dar, die ohne Rechtsgrundlage erfolgte:

- Sie konnte nicht auf §§ 46 Abs. 1 Ordnungswidrigkeitengesetz i.V.m. 163 Abs. 1 StPO gestützt werden. Diese Vorschriften regeln die Befugnis der Ordnungswidrigkeitenbehörden, zur Aufklärung der zu Grunde liegenden Ordnungswidrigkeit andere Behörden um Auskunft zu ersuchen sowie grundsätzlich Ermittlungen jeder Art vorzunehmen. Das Schreiben an die Bank stand jedoch in keinem Zusammenhang mit der Aufklärung der Ordnungswidrigkeit.

- Ebenfalls nicht einschlägig waren die §§ 46 Abs. 1 Ordnungswidrigkeitengesetz i.V.m. § 475 Abs. 1, 4 StPO, die unter bestimmten Voraussetzungen im Ordnungswidrigkeitenverfahren Datenübermittlungen an Privatpersonen zulassen. Diese Regelungen betreffen aber ausschließlich Fälle, in denen die Datenübermittlungen im Interesse der privaten Empfänger erfolgen. Dies war hier aber nicht der Fall.

- Die Übermittlung konnte auch nicht auf Art. 19 BayDSG gestützt werden. Nach dieser Vorschrift ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn sie u.a. zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Dies war hier jedoch nicht der Fall, da dem Polizeipräsidium Möglichkeiten zur Verfügung standen, sich ohne Einschaltung Dritter mit dem Betroffenen in Verbindung zu setzen. Nachdem die Zahlung auf die Übersendung eines Anhö-

rungsbogens an die GmbH hin erfolgt war, musste das Polizeipräsidium davon ausgehen, dass der Betroffene über die GmbH - deren Anschrift der Polizei bekannt war - erreicht werden konnte. Das Polizeipräsidium hätte daher den Betroffenen über die GmbH anschreiben können.

- Nachdem datenschutzrechtlich unbedenkliche Möglichkeiten bestanden, den Betroffenen zeitnah zu erreichen, konnte die Datenübermittlung - auch wenn sie mit dem Zweck erfolgte, die Einleitung eines Bußgeldverfahrens, das für den Betroffenen mit weiteren Kosten verbunden gewesen wäre, zu vermeiden - auch nicht auf seine mutmaßliche Einwilligung gestützt werden.

Ich habe diese Datenübermittlung förmlich beanstandet und das Polizeipräsidium aufgefordert, sich in zukünftigen vergleichbaren Fällen, in denen eine Abklärung mit dem Einzahler eines Buß- bzw. Verwarnungsgeldes erforderlich ist, unmittelbar mit dem Einzahler in Verbindung zu setzen.

9.5.5 Übersendung einer Liste von Betroffenen

Ein Rechtsanwalt hatte sich mit folgendem Sachverhalt an mich gewandt: Gegen seine Mandantin war ein Ordnungswidrigkeitenverfahren wegen eines Parkverstoßes eingeleitet worden. Auf ihren Einspruch hin war das Verfahren eingestellt worden, nachdem sich nicht klären ließ, wer den PKW verbotswidrig geparkt hatte. Der Betroffenen waren jedoch die Kosten des Verfahrens auferlegt worden. Gegen diese Entscheidung hatte der Verteidiger Antrag auf gerichtliche Entscheidung gestellt. Daraufhin hatte die Ordnungswidrigkeitenbehörde dem zuständigen Amtsgericht die Verfahrensunterlagen übersandt, bei denen sich - einschließlich der Betroffenen - eine Auflistung aller Fahrzeughalter befand, die am selben Tag eine schriftliche Verwarnung erhalten hatten. Diese Auflistung, die insgesamt 39 Vorgänge umfasste, hatte neben der Verwarnungsnummer jeweils den Namen und den Vornamen des betroffenen Kfz-Halters sowie die sog. Halternummer, die einen EDV-Schlüssel der vollständigen Personalien darstellt, enthalten.

Da das Amtsgericht für die Entscheidung über die Kostentragung zuständig ist, war zwar die Übersendung der Unterlagen, die sich auf die Betroffene bezogen, zulässig. Die Zulässigkeit der Übermittlung der Daten der weiteren in der Liste genannten Personen richtet sich nach Art. 18 Abs. 4 Satz 1 BayDSG. Eine derartige Datenübermittlung ist danach nur zulässig, wenn eine Trennung der Daten nicht oder nur mit unvertretbarem Aufwand möglich ist und nicht offensichtlich überwiegende schutzwürdige Interessen des Betroffenen oder Dritter entgegenstehen. Hier war eine Trennung (durch Schwärzung der übrigen auf der Liste enthaltenen Namen und Daten) mit vertretbarem Aufwand möglich, so dass die Übermittlung dieser Daten von der Ordnungswidrigkeitenbehörde an das Amtsgericht unzulässig war.

Ich habe die Ordnungswidrigkeitenbehörde deshalb förmlich beanstandet und aufgefordert, in zukünftigen Fällen Daten solcher für das Ordnungswidrigkeitenverfahren nicht relevanter Personen vor der Übermittlung unkenntlich zu machen.

10 Vermessungsverwaltung

10.1 Amtliches Liegenschaftskataster-Informationssystem „ALKIS“

Antragsteller auf Erteilung einer Baugenehmigung müssen mit dem Bauantrag bei der Gemeinde nach Art. 67 Abs. 2 Bayerische Bauordnung i.V.m. §§ 1 ff. Bauvorlagenverordnung bestimmte Unterlagen (sog. Bauvorlagen) einreichen. Zu diesen Unterlagen gehört auch ein auf einer Ablichtung des Auszugs aus dem Katasterkartenwerk zu erstellender Lageplan. Dieser muss, soweit für die Beurteilung des Vorhabens erforderlich, u.a. die katastermäßige Bezeichnung des Baugrundstücks und der benachbarten Grundstücke mit Angabe der Eigentümer und, soweit vorhanden, der Straße und der Hausnummer enthalten.

Ein Grundstückseigentümer hatte sich an mich gewandt, weil in dem vom Vermessungsamt erteilten Auszug zur Bauvorlage u.a. auch die Miteigentumsanteile der Grundstückseigentümer angegeben waren.

Da der Bauherr verpflichtet ist, mit seinem Bauantrag einen Lageplan mit bestimmten Angaben einzureichen, hat er insoweit ein berechtigtes Interesse an der Erteilung eines Auszugs aus dem Liegenschaftskataster. Dies gilt jedoch nicht für die Angabe der Eigentumsanteile der jeweiligen Eigentümer der Nachbargrundstücke, da diese Daten für die Stellung eines Bauantrags nicht erforderlich sind.

Nachdem mir das zuständige Vermessungsamt mitgeteilt hatte, der Inhalt derartiger Auszüge sei durch die Vermessungsämter nicht beeinflussbar, da er durch das Programm „ALKIS“ vorgegeben sei, habe ich mich an das für Änderungen der Programmierung zuständige Staatsministerium der Finanzen gewandt. Dieses hat die bisherige Verfahrensweise dahingehend umgestellt, dass in den Auszügen aus dem Lie-

genschaftskataster zur Bauvorlage nur noch die Eigentümer der Nachbargrundstücke, nicht jedoch deren Miteigentumsanteile ausgewiesen werden.

11 Gemeinden, Städte und Landkreise

11.1 Gesetz zur Stärkung elektronischer Verwaltungstätigkeit

Am 1.2.2003 ist das Gesetz zur Stärkung elektronischer Verwaltungstätigkeit vom 24.12.2002 in Kraft getreten. Das Gesetz schafft den rechtlichen Rahmen für eine rechtsverbindliche elektronische Kommunikation zwischen Bürger und Verwaltung. Dazu wurden das Bayerische Verwaltungsverfahrensgesetz (BayVwVfG) und die Fachgesetze des besonderen Verwaltungsrechts grundsätzlich auch insoweit, als bisher die schriftliche Form vorgeschrieben war, für die Möglichkeit der elektronischen Kommunikation mit der Folge geöffnet, dass die Schriftform nunmehr durch die elektronische Form in Verbindung mit einer qualifizierten elektronischen Signatur ersetzt werden kann. Das Gesetz enthält die dafür notwendigen Maßgaben und Anpassungen sowie einige Ausnahmeregelungen. Zugleich setzt das Gesetz Änderungen des Melderechtsrahmengesetzes in Landesrecht um.

Das Gesetz enthält insbesondere folgende, aus datenschutzrechtlicher Sicht wesentliche Änderungen:

1. Änderung des Bayerischen Verwaltungsverfahrensgesetzes

a) Nach der neuen Regelung des Art. 3 a Abs. 1 BayVwVfG ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet

In das Bayerische Verwaltungsverfahrensgesetz wurde ein neuer Art. 3 a eingefügt. Er regelt in Abs. 1 die Zulässigkeit der Übermittlung elektronischer Dokumente. Diese ist danach zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. Dazu müssen zunächst die technischen und personellen Voraussetzungen geschaffen werden. Hinzu kommen muss der Wille zur Eröffnung eines Zugangs, d.h. der Empfänger muss den Zugang erst durch eine entsprechende Widmung eröffnen. Dies kann ausdrücklich oder konkludent erfolgen. Im Einzelnen wird hier die Verkehrsanschauung maßgebend sein. Nach der Gesetzesbegründung wird zur Zeit beim Bürger im Verkehr mit Behörden in aller Regel von der Eröffnung eines Zugangs für den Empfang elektronischer Dokumente, an deren Zugang sich rechtliche Folgen knüpfen, nur dann ausgegangen werden können, wenn er dies gegenüber der Behörde ausdrücklich erklärt hat. Die Behörden, die auf ihren Briefköpfen im Verkehr mit dem Bürger oder der Verwaltung eine E-Mail-Adresse angeben, erklären damit konkludent ihre Bereitschaft, Eingänge auf diesem Weg anzunehmen. Da jedenfalls derzeit die Angabe einer E-Mail-Adresse aber noch nicht ohne weiteres auf die Eröffnung eines Zugangs für den Empfang von (signierten) Dokumenten in elektronischer Form schließen lässt, wird in der Gesetzesbegründung empfohlen, die Voraussetzungen für den Empfang elektronischer Dokumente durch Hinweise auf dem Briefkopf und auf der Internetseite klarzustellen. Dabei kann die Zugangseröffnung auf bestimmte Verfahren und bestimmte technische Standards beschränkt werden. Wenn Behörden einen Zugang für den Empfang von elektronischen Dokumenten eröffnet haben, dann müssen sie durch organisatorische Maßnahmen sicherstellen, dass z.B. E-Mail-Postfächer regelmäßig abgefragt werden. In der Gesetzesbegründung wird allerdings klargestellt, dass die neue Regelung des Art. 3 a keinen rechtlichen oder tatsächlichen Zwang auf Behörden und/oder Bürger zur Schaffung der Voraussetzungen für eine moderne elektronische Kommunikation ausübt.

b) Art. 3 a Abs. 2 Sätze 1 und 2 BayVwVfG regeln, dass ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist, gesetzlichen angeordneten Schriftformerfordernissen genügt

In der Gesetzesbegründung wird dazu ausgeführt, dass der Verweis auf die qualifizierte elektronische Signatur im Sinne des Signaturgesetzes die Funktionen der Schriftform (Abschlussfunktion, Perpetuierungsfunktion, Identitätsfunktion, Echtheitsfunktion, Verifikationsfunktion, Beweisfunktion und

Warnfunktion) für den Bereich der elektronischen Kommunikation in ihrer Gesamtheit sicherstellt.

c) Art. 30 BayVwVfG fordert die Sicherstellung der Vertraulichkeit elektronischer Dokumente

Mit dem Erfordernis einer qualifizierten elektronischen Signatur nach dem Signaturgesetz in Art. 3 a Abs. 2 Satz 2 BayVwVfG werden lediglich die Integrität (d.h. dass personenbezogene Daten vollständig und unverfälscht vorliegen bzw. beim Empfänger ankommen) und die Authentizität (d.h. dass personenbezogene Daten zweifelsfrei ihrem Ursprung zugeordnet werden können) elektronischer Dokumente sichergestellt. Die Vertraulichkeit der bei der elektronischen Kommunikation übertragenen Daten (d.h. dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können) ist im Gesetz hingegen nicht ausdrücklich geregelt. Nach der Gesetzesbegründung ist dies auch nicht erforderlich, da die Behörde nach Art. 30 BayVwVfG die notwendigen Sicherheitsvorkehrungen treffen, also etwa elektronische Dokumente in geeigneter Weise verschlüsseln muss. Auch ohne ausdrückliche gesetzliche Regelung in Art. 3 a BayVwVfG hat danach die Behörde bei der Übermittlung elektronischer Dokumente zu gewährleisten, dass dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung der Vertraulichkeit der übertragenen Daten getroffen werden.

d) Art. 3 a Abs. 2 Satz 3 BayVwVfG schließt die Signatur mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, aus

§ 7 Abs. 1 Nr. 1 des Signaturgesetzes eröffnet die Möglichkeit der Zuordnung von Signaturen an Personen unter einem Pseudonym. Die Regelung in Art. 3 a Abs. 2 Satz 3 BayVwVfG ist daher erforderlich, um eine missbräuchliche Inanspruchnahme der Verwaltung durch eine Pseudonymverwendung, die keine Identifizierung ermöglicht, auszuschließen. Nach der Gesetzesbegründung ist jedoch die Signierung durch eine erlassene Behörde - ohne Nennung des Bearbeiters - mittels einer Sachbezeichnung (z.B. Stadt XY) zulässig.

e) Verfahren bei nicht kompatiblen Kommunikationsmethoden

Art. 3 a Abs. 3 BayVwVfG regelt den Fall, dass die verwendeten Kommunikationsmethoden zueinander nicht kompatibel sind, so dass Bürger oder Behörde übermittelte elektronische Dokumente nicht lesen und damit nicht bearbeiten können. Die Behörde, die ein Dokument erhält, das für sie zur Bearbeitung nicht geeignet ist, hat dies dem Absender mit Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen. Macht der Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

f) Weitere wichtige Änderungen:

- Nach Art. 15 Satz 2 BayVwVfG wird für den Fall, dass ein Beteiligter ohne Wohnsitz oder gewöhnlichen Aufenthalt, Sitz oder Geschäftsleitung im Geltungsbereich des Grundgesetzes der Behörde auf Verlangen innerhalb einer angemessenen Frist keinen Empfangsbevollmächtigten im Geltungsbereich des Grundgesetzes benannt hat, bei der Übermittlung eines elektronischen Dokuments der Zugang am dritten Tag nach der Übermittlung vermutet. Art. 15 Satz 2 ist allerdings nur anwendbar, wenn der Behörde der ausländische Wohnsitz oder Aufenthaltsort oder Sitz bekannt ist.

- Art. 37 BayVwVfG regelt, dass ein Verwaltungsakt auch in elektronischer Form erlassen werden kann und dass die inhaltlichen Anforderungen an elektronische Verwaltungsakte denen an schriftliche Verwaltungsakte entsprechen. Die Vorschrift stellt außerdem klar, dass ein mündlicher Verwaltungsakt schriftlich oder elektronisch

bestätigt werden kann. Die Vorschrift sieht außerdem die Möglichkeit der Anordnung der dauerhaften Überprüfbarkeit der qualifizierten elektronischen Signatur vor.

- Art. 39 BayVwVfG regelt, dass auch ein elektronischer Verwaltungsakt mit einer Begründung zu versehen ist.

- Nach Art. 41 BayVwVfG gilt ein Verwaltungsakt, der elektronisch übermittelt wird, am dritten Tag nach der Absendung als bekannt gegeben. In der Vorschrift wird außerdem klar gestellt, dass die Regelung über die öffentliche Bekanntgabe eines Verwaltungsaktes auch für elektronische Verwaltungsakte gilt.

- In Art. 66 BayVwVfG wird klargestellt, dass den Beteiligten auch ein der Behörde elektronisch vorliegendes Gutachten zugänglich gemacht wird.

- In Art. 69 BayVwVfG wird geregelt, dass ein elektronischer Verwaltungsakt in einem förmlichen Verwaltungsverfahren mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur zu versehen ist und dass der beteiligte Bürger den Verwaltungsakt auch in einfacher elektronischer Form anfordern kann.

2. Wichtige Änderungen der Gemeindeordnung

- Nach Art. 18 a Abs. 18 GO findet das elektronische Verfahren bei Bürgerbegehren und Bürgerentscheid keine Anwendung. In der Begründung wird dazu ausgeführt, dass eine elektronische Form z.B. bei den Unterschriften beim Bürgerbegehren nicht möglich ist, da die Unterschriften unter der Fragestellung und Begründung von den Initiatoren privat gesammelt werden müssen und dann grundsätzlich alle einheitlich bei der Gemeinde abzugeben sind. Eine Zusammenfassung einzeln eingehender elektronisch signierter Unterschriften würde einen enormen Verwaltungsaufwand bedeuten und außerdem zu nicht akzeptabeln Unsicherheiten hinsichtlich des eingereichten Antrags und dem Erreichen des Quorums führen. Der Bürgerentscheid selbst wird ähnlich wie eine Wahl abgewickelt. Insoweit ist wegen der Höchstpersönlichkeit der wahlähnlichen Entscheidung und ihrer Bedeutung die elektronische Form nicht sinnvoll.

- Nach Art. 18 b Abs. 8 GO scheidet ein elektronisches Verfahren auch beim Bürgerantrag aus. Es gelten hier grundsätzlich die gleichen Überlegungen wie beim Bürgerbegehren.

3. Änderung des Meldegesetzes

Das Melderechtsrahmengesetz vom 25.3.2002 sieht unter anderem eine elektronische Selbstauskunft, eine elektronische Anmeldung und eine elektronische einfache Melderegisterauskunft vor. Im Einzelnen verweise ich dazu auf meine Ausführungen im 20. Tätigkeitsbericht unter der Nr. 10.1. Diese Neuregelungen wurden mit der Änderung des Meldegesetzes in Bayerisches Landesgesetz umgesetzt (Art. 9 Abs. 1 a, Art. 17 Abs. 1 Satz 2 und Art. 34 Abs. 1 a MeldeG. In das Meldegesetz wurde ein neuer Art. 43 eingefügt mit dem das Staatsministerium des Innern ermächtigt wird, die Einzelheiten der genannten Verfahren durch Rechtsverordnung festzulegen. Die Umsetzung weiterer Änderungen des Melderechtsrahmengesetzes in das Bayerische Meldegesetz (u.a. elektronische Rückmeldung und elektronische Datenübermittlung an andere Behörden) wird zur Zeit vorbereitet.

11.2 Übertragung öffentlicher Gemeinderatssitzungen im Internet

Durch die Eingabe eines betroffenen Gemeinderatsmitglieds ist mir folgender Sachverhalt bekannt geworden:

Eine Kommune übertrug eine öffentliche Sitzung ihres Gemeinderats live im Internet. Zu Beginn der Sitzung fragte der erste Bürgermeister in Anwesenheit der Öffentlichkeit und bei laufender Kamera, ob alle Mitglieder des Gemeinderats mit der Internetübertragung einverstanden sind. Daraufhin verweigerten drei Gemeinderatsmitglieder ihre Zustimmung. Im Folgenden wurden dann zwar von diesen Gemeinderatsmitgliedern keine Bilder im Internet gezeigt, der Wortlaut ihrer Redebeiträge wurde je-

doch ausgestrahlt. Nach Prüfung der Angelegenheit und einer grundsätzlichen Besprechung mit dem Bayerischen Staatsministerium des Innern vertrete ich dazu zusammengefasst die folgende Auffassung:

Eine Übertragung der Sitzungsbeiträge von Gemeinderatsmitgliedern oder Redebeiträgen von Gemeindebediensteten im Internet ist nur zulässig, wenn diese der Übertragung zugestimmt haben und zwar sowohl was Bild, wie was Ton betrifft.

Die Entscheidung über die Zustimmung muss ohne psychischen Druck auf der Grundlage ausreichender Informationen über die besonderen Modalitäten einer Interneteinstellung und mit ausreichender Überlegungsfrist erfolgen können.

Die Verweigerung der Zustimmung darf nicht in diskriminierender Weise zur Kenntnis gebracht werden.

Der Zuschauerraum darf nicht so in die Übertragung einbezogen werden, dass einzelne Zuschauer erkannt werden können.

Im Einzelnen waren folgende Erwägungen für diese Beurteilung maßgebend:

1. Soweit ersichtlich haben sich Rechtsprechung und Literatur mangels eines konkreten Anlasses bisher noch nicht zur Zulässigkeit von Liveübertragungen öffentlicher Gemeinderatssitzungen durch Kommunen im Internet geäußert.

   Herangezogen werden können jedoch Rechtsprechung und Literatur zu Film- und Tonbandaufnahmen:

   Zu Tonbandaufzeichnungen durch Pressevertreter oder sonstige Besucher in öffentlichen Sitzungen wird zum Teil die Auffassung vertreten, das einzelne Gemeinderatsmitglied könne das Abschalten des Tonbandgeräts während seines Redebeitrags nicht verlangen, weil es hier nicht als „Privatperson“ rede und bei öffentlichen Verhandlungen vor kommunalen Organen gehaltene Reden im Sinn des § 48 Abs. 1 Nr. 2 UrhG auch urheberrechtlich nicht geschützt seien (vgl. Bauer/Böhle/Masson/Samper, Bayerische Gemeindeordnung, Art. 52 Rdnr. 8 mit weiteren Nachweisen). Demgegenüber folgern Widtmann/Grasser, Bayerische Gemeindeordnung, Art. 52 Rdnr. 10, aus dem Urteil des Bundesverwaltungsgerichts vom 03.08.1990 (BayVBl 1991, 89) zu Recht, dass Bild- und Tonaufzeichnungen nicht nur eines Gemeinderatsbeschlusses bedürfen, sondern jedes einzelne ehrenamtliche Gemeinderatsmitglied sich der Aufnahme während seines Redebeitrags widersetzen kann mit der Folge, dass der Vorsitzende die Aufnahme dieses Redebeitrags zu untersagen hat (im Ergebnis ebenso u.a. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Teil C Handbuch, Abschnitt XII Nr. 5 Buchst. b sowie Antwort des StMI auf eine schriftliche Anfrage im Bayerischen Landtag vom 16.04.87/06.05.87, LT-Drs. 11/1697, Stemmer, KommunalPraxis BY 1987, 86 und Keller, KommunalPraxis BY 2000, 412, die außerdem noch die Zustimmung des Vorsitzenden im Gemeinderat, also regelmäßig des ersten Bürgermeisters, fordern). In dem zitierten Urteil hat das Bundesverwaltungsgericht entschieden, dass die Pressefreiheit nicht dadurch verletzt wird, dass ein Ratsvorsitzender in Ausführung eines entsprechenden Ratsbeschlusses einem Journalisten untersagt, die öffentliche Sitzung des Rates auf Tonband aufzuzeichnen. In der Begründung führt das Bundesverwaltungsgericht aus, das Recht des Ratsmitglieds auf freie Rede könne durch die Aufzeichnung auf Tonband faktisch empfindlich tangiert werden. Eine von psychologischen Hemmnissen möglichst unbeeinträchtigte Atmosphäre gehöre zu den notwendigen Voraussetzungen eines geordneten Sitzungsbetriebs, den der Ratsvorsitzende zu gewährleisten habe.

   Zu diesen vom Bundesverwaltungsgericht zu Tonaufnahmen geäußerten Bedenken kommt bei Fernsehaufnahmen noch das Bild dazu. Der Eingriff in das Persönlichkeitsrecht des einzelnen Gemeinderatsmitglieds ist hier noch umfassender und stärker als bei reinen Tonaufnahmen (vgl. Stemmer, a.a.O., S. 88).

2. Die Direktübertragung von öffentlichen Gemeinderatssitzungen im Internet stellt datenschutzrechtlich eine Übermittlung personenbezogener Daten weltweit an eine Vielzahl unbestimmter Personen dar. Betroffen sind dabei nicht nur die Gemeinderatsmitglieder und sonstige Personen (z.B. Gemeindebedienstete). Betroffen sind auch Bürger, deren Angelegenheiten in einer solchen Gemeinderatssitzung personenbezogen behandelt werden. Schließlich sind auch Zuhörer betroffen, wenn sie auf den im Internet verbreiteten Aufnahmen erkennbar sind oder ein Rückschluss auf ihre Person möglich ist.

   Die Erhebung personenbezogener Daten und ihre Übermittlung über das Internet sind nur zulässig, wenn entweder das Bayerische Datenschutzgesetz (BayDSG) oder eine andere

Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat (Art. 15 Abs. 1 Nrn. 1 und 2 BayDSG).

a) Auf Art. 52 Abs. 2 Satz 1 der Gemeindeordnung (GO) kann eine Übertragung öffentlicher Gemeinderatssitzungen im Internet nicht gestützt werden. Aus dieser Vorschrift ergibt sich zwar, dass Gemeinderatssitzungen grundsätzlich öffentlich abzuhalten sind. Damit wird die Transparenz kommunaler Verwaltungstätigkeit gewährleistet. Öffentlichkeit der Sitzungen bedeutet aber nur, dass jedermann im Rahmen des hierfür zur Verfügung stehenden Platzes in der Reihenfolge des Eintreffens freien Zugang zum Sitzungsraum hat (vgl. Bauer/Böhle/Masson/Samper, a.a.O., Art. 52 Rdnr. 7 sowie Widtmann/Grasser, a.a.O., Art. 52 Rdnr. 8). Die Gemeinderatsmitglieder und sonstige Personen, die an der Sitzung teilnehmen, z.B. Gemeindebedienstete, die zu einem Tagesordnungspunkt berichten, sowie Bürger, deren Angelegenheiten personenbezogen in der Sitzung behandelt werden, müssen es daher nach Art. 52 Abs. 2 Satz 1 GO nur hinnehmen, dass Zuhörer der Sitzung beiwohnen, sich ggf. Notizen machen und anschließend in der Presse berichtet wird. Für einen darüber hinaus gehenden Eingriff in ihr informationelles Selbstbestimmungsrecht dergestalt, dass die Sitzung in Bild und Ton im Internet übertragen wird, stellt Art. 52 Abs. 2 Satz 1 GO keine Rechtsgrundlage dar (so auch Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, Teil C, Handbuch XII.5.c).

   Bei einer Übertragung im Internet ist auch zu berücksichtigen, dass damit eine völlig neue Qualität der Veröffentlichung vorgenommen wird. Die Veröffentlichung im Internet erreicht weltweit einen ungleich größeren Personenkreis als jede auflagenbegrenzte schriftliche Presseveröffentlichung oder die Berichterstattung in einem lokalen Rundfunksender. Bild und Ton können von jedermann abgerufen, aufgezeichnet und ausgewertet werden und die weitere Verwendung dieser Aufnahme ist nicht abzusehen. Bei einer Direktübertragung von öffentlichen Gemeinderatssitzungen im Internet werden außerdem die Betroffenen mit ihrer Mimik und Gestik sowie ihre Redebeiträge im Wortlaut weltweit abrufbar. Dies kann dazu führen, dass sich ehrenamtliche Gemeinderatsmitglieder nicht mehr unbefangen und spontan äußern (vgl. BVerwG a.a.O.). Dadurch aber würde die Funktionsfähigkeit des Gemeinderats beeinträchtigt und der Demokratie insgesamt Schaden zugefügt.

b) Für die Übertragung von Gemeinderatssitzungen im Internet kann nicht Art. 19 Abs. 1 Nr. 2 BayDSG als Rechtsgrundlage herangezogen werden. Nach dieser Vorschrift 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. Es ist bereits fraglich, ob Art. 19 Abs. 1 Nr. 2 BayDSG hier neben Art. 52 Abs. 2 GO, der die Öffentlichkeit bzw. Nichtöffentlichkeit der Gemeinderatssitzungen bereichsspezifisch regelt, anwendbar ist (vgl. Wilde/Ehmann/Niese/Knoblauch, a.a.O., Teil C Handbuch, Abschnitt XII Nr. 2 Buchst. b). Ungeachtet dessen sind auch die Voraussetzungen dieser Vorschrift nicht erfüllt, da ein berechtigtes Interesse der Öffentlichkeit an einer weltweiten Übertragung von Gemeinderatssitzungen im Internet nicht besteht und die davon Betroffenen ein schutzwürdiges Interesse haben, dass ihre personenbezogenen Daten nur im gesetzlichen Rahmen des Art. 52 Abs. 2 Satz 1 GO an Dritte übermittelt werden. Sie haben außerdem auch ein schutzwürdiges Interesse daran, dass ihre personenbezogenen Daten nicht ohne ihre Einwilligung in Drittländer übermittelt werden, in denen kein angemessenes Datenschutzniveau gewährleistet ist (Art. 21 Abs. 2 Satz 2 BayDSG).

c) Bei einer Übertragung öffentlicher Gemeinderatssitzungen im Internet dürfen daher aus datenschutzrechtlicher Sicht nur die Personen in Wort und Bild aufgenommen werden, die vorher in die Übertragung eingewilligt haben (Art. 15 Abs. 1 Nr. 2 BayDSG). Die

betroffenen Personen sind darauf hinzuweisen, dass bei einer Übertragung im Internet Bild und Ton weltweit von einem unbegrenzten Kreis von Personen abgerufen, aufgezeichnet, unter Umständen verändert und ausgewertet werden können und die weitere Verwendung dieser Aufnahmen nicht abzusehen ist (Grundsatz der informierten Einwilligung, vgl. Art. 15 Abs. 2 BayDSG). Sie dürfen dabei nicht unter einen Entscheidungsdruck gesetzt werden. Das wäre z.B. der Fall, wenn sie in der Öffentlichkeit im Beisein von Zuhörern und der Presse, mit dem Wunsch nach einer Übertragung der Gemeinderatssitzung im Internet konfrontiert würden. Von einer freiwilligen Einwilligung könnte in einem solchen Fall nicht ausgegangen werden. Es muss den Betroffenen daher eine angemessene Überlegungsfrist für ihre Entscheidung eingeräumt werden. Die Einwilligung muss außerdem jederzeit ohne Angabe von Gründen widerrufen werden können. Dies gilt auch für Bürger, deren Angelegenheiten personenbezogen bzw. personenbeziehbar in öffentlicher Gemeinderatssitzung behandelt und im Internet übertragen werden sollen.

Im Ergebnis bedeutet dies, dass an Stelle eines **Gemeindebediensteten**, der in die Übertragung im Internet nicht eingewilligt hat, ein anderer Mitarbeiter der Gemeinde oder ggf. der erste Bürgermeister den zu einem Tagesordnungspunkt vorgesehenen Bericht der Verwaltung übernehmen muss. **Bürgerangelegenheiten,** die dem Datenschutz unterliegen, dürfen ohne Einwilligung des Betroffenen in öffentlicher Gemeinderatssitzung ohnehin nur anonymisiert behandelt werden. Verweigert ein **Gemeinderatsmitglied** seine Einwilligung in die Übertragung, dürfen seine Redebeiträge weder in Bild noch in Ton übertragen werden. Bei einer Liveübertragung im Internet bedeutet dies, dass, da die entsprechenden Sequenzen aus der Aufnahme nicht herausgeschnitten werden können, diese Zeitabschnitte überbrückt werden müssen. Dabei ist zu vermeiden, dass bei jedem Redebeitrag die Verweigerung des Gemeinderatsmitglieds jedes Mal aufs Neue öffentlich dokumentiert wird. Dies kann sich auf das Gemeinderatsmitglied erheblich belastend auswirken, insbesondere, wenn wie im vorliegenden Fall in der Presse mit Überschriften wie „Kamerascheue Politiker“ und „Drei CSUler wollten nicht ins Bild“ darüber berichtet wird.

Man könnte deshalb in Erwägung ziehen, bei der Verweigerung eines Gemeinderatsmitglieds die Zulässigkeit einer Übertragung der Gemeinderatssitzung im Internet insgesamt in Zweifel zu ziehen, weil anderenfalls wegen der zu befürchtenden Drucksituation für das Gemeinderatsmitglied eine freiwillige Entscheidung nicht gewährleistet wäre.

Andererseits muss aber auch berücksichtigt werden, dass dann unter Umständen ein einziges Gemeinderatsmitglied gegen den erklärten Willen aller anderen Gemeinderatsmitglieder eine Einstellung der öffentlichen Sitzung in das Internet verhindern könnte und der öffentliche Druck auf den Verweigerer mindestens genauso groß wäre. Ich halte eine Internetübertragung angesichts dessen trotzdem für vertretbar, wenn der Weigerung eines Gemeinderatsmitglieds dadurch Rechnung getragen wird, dass seine Redebeiträge in Wort und Bild aus der Übertragung ausgeblendet werden und die Dokumentierung seiner Weigerung durch entsprechende Aufnahmetechniken vermieden wird. Gegebenenfalls ist anstatt einer Liveübertragung eine Aufzeichnung ins Internet einzustellen.

d) Der Zuhörerbereich ist von einer Übertragung im Internet auszunehmen, da es hier den Umständen nach nicht möglich ist, von den einzelnen Zuhörern eine rechtswirksame Einwilligung einzuholen. Eine entsprechende Frage in den Zuhörerraum vor Beginn der Sitzung würde den Anforderungen an eine Einwilligung im Sinn des Art. 15 Abs. 2 und 3 BayDSG nicht genügen.

3. In dem zu entscheidenden Fall hat der erste Bürgermeister erst zu Beginn der Gemeinderatssitzung in Anwesenheit der Öffentlichkeit und bei laufender Kamera gefragt, ob alle Mitglieder des Gemeinderats mit der Internetübertragung einverstanden sind. Im Folgenden wurden dann zwar von den Gemeinderatsmit-

gliedern, die ihre Einwilligung in die Übertragung verweigert haben, keine Bilder gezeigt, der Wortlaut ihrer Beiträge wurde jedoch ausgestrahlt. Damit lag ein Verstoß gegen datenschutzrechtliche Bestimmungen vor; die Gemeinderatsmitglieder hätten rechtzeitig vor Beginn der öffentlichen Sitzung zu ihrer Einwilligung befragt und dabei über die Folgen der Übertragung aufgeklärt werden müssen. Der Wortlaut der Redebeiträge der Gemeinderatsmitglieder, die ihre Einwilligung in die Übertragung im Internet nicht erteilt haben, hätte nicht ausgestrahlt werden dürfen. Da der erste Bürgermeister jedoch im guten Glauben war, den datenschutzrechtlichen Anforderungen zu genügen und er wenigstens die Bilder der Gemeinderatsmitglieder, die ihre Zustimmung verweigert haben, ausgeblendet hat, habe ich im Rahmen meines Ermessens nach Art. 31 Abs. 3 BayDSG für dieses Mal von einer Beanstandung abgesehen.

11.3 Veröffentlichung von Personenstandsdaten im Internet

Ein Bürger hat sich an mich mit dem Vorbringen gewandt, auf der Internetseite einer Gemeinde würden Vor- und Nachname sowie Geburtsdatum seiner Tochter ohne seine Zustimmung veröffentlicht. Bei der von mir daraufhin durchgeführten Überprüfung habe ich festgestellt, dass die Gemeinde auf ihrer Homepage sämtliche Geburten, Eheschließungen und Sterbefälle des laufenden Jahres 2003 sowie alle Geburten, Eheschließungen und Sterbefälle der Jahre 1998 bis 2002 veröffentlicht hatte. Meiner Aufforderung, die personenbezogenen Daten von der Homepage zu entfernen, für deren Veröffentlichung keine Einwilligungen vorlagen, ist die Gemeinde sofort nachgekommen. Von einer förmlichen Beanstandung konnte ich gleichwohl nicht absehen, da es sich bei der Veröffentlichung in dem hier beurteilten Fall um einen erheblichen Datenschutzverstoß handelte. Im Einzelnen weise ich dazu auf Folgendes hin:

Die Veröffentlichung von Geburten, Eheschließungen und Sterbefällen im Internet stellt eine Datenübermittlung im Sinn des Art. 4 Abs. 6 Satz 2 Nr. 3 BayDSG dar. Mangels einer Rechtsvorschrift, die eine derartige Veröffentlichung erlaubt, ist diese nur dann zulässig, wenn die Betroffenen, bei Sterbefällen die Angehörigen, darin eingewilligt haben (Art. 15 Abs. 1 BayDSG). Die betroffenen Bürger müssen dabei informiert werden, für welchen Zeitraum und auf welches Medium (z.B. Veröffentlichung im Amtsblatt, in der Tageszeitung, auf der gemeindlichen Homepage) sich die Einwilligung bezieht. So sind bspw. die Betroffenen, die der Veröffentlichung ihrer Daten im Amtsblatt zustimmen, auch darüber zu informieren, dass das Amtsblatt mit diesen Daten zusätzlich auf der Homepage der Gemeinde eingesehen werden kann.

11.4 Veröffentlichung der Anschriften von Vereinen auf der Homepage der Gemeinde

Im Berichtszeitraum bin ich mehrmals gefragt worden, ob Gemeinden die Anschriften, die ihnen ihre Vereine mitteilen, auf ihrer Homepage veröffentlichen dürfen. Ich vertrete dazu die folgende Auffassung:

Die Veröffentlichung der Anschriften von Vereinen auf der Homepage der jeweiligen Gemeinde ist regelmäßig ohne Zustimmung der Vereine zulässig. Dies gilt auch dann, wenn - wie bei kleinen Vereinen üblich - der Verein unter der Anschrift des Vereinsvorsitzenden zu erreichen ist (vgl. Wilde/Ehmann/Niese/Knoblauch, Kommentar zum Bayerischen Datenschutzgesetz, Teil C Handbuch, XII.8.a) cc)). Die Vereinsanschrift ist regelmäßig ein offenkundiges, nach dem Willen der Beteiligten auf Kenntnis und Verbreitung in der Öffentlichkeit angelegtes Datum und deshalb nicht schutzbedürftig. Soweit jedoch über die Bekanntgabe der Vereinsanschrift hinausgehende Veröffentlichungen beabsichtigt sind (z.B. die der privaten Telefonnummer von Vorstandsmitgliedern etc.), ist dies nur mit Einwilligung der Betroffenen zulässig (vgl. Art. 15 Abs. 1 Nr. 2 BayDSG).

Die Bekanntgabe von Anschriften der Vereine durch die Gemeinde dient dazu, den Bürgern die Kontaktaufnahme mit den örtlichen Vereinen zu erleichtern. In aller Regel haben die Vereine ein eigenes Interesse daran, dass ihre Kontaktadressen den Bürgern bekannt sind und hierzu von der Gemeinde veröffentlicht werden. Von der Veröffentlichung muss die Gemeinde daher in diesen Fällen nur auf ausdrücklichen Wunsch eines Vereins absehen. Bei Zweifeln am Veröffentlichungsinteresse des Vereins sollte dessen Einwilligung eingeholt werden.

11.5 Veröffentlichung von Bauherrendaten im Internet

Nach Art. 84 der Bayerischen Bauordnung (BayBO) dürfen die Bauaufsichtsbehörden und die Gemeinden Ort und Straße der Baustelle, Art und Größe des Bauvorhabens sowie Namen und Anschrift des Bauherren und des Entwurfsverfassers veröffentlichen oder an Dritte zum Zwecke der Veröffentlichung übermitteln, wenn der Betroffene der Veröffentlichung nicht widersprochen hat. Der Betroffene ist bei

der Bauantragsstellung auf sein Widerspruchsrecht hinzuweisen. Die vom Bayerischen Staatsministerium des Innern im Vollzug von § 6 Abs. 2 der Bauvorlagenverordnung mit Bekanntmachung vom 28.12.1999 (AllMBl 2000 S. 6) bekannt gemachten und verbindlich eingeführten Vordrucke sehen dazu in der Anlage 1 (Bauantrag und Abgrabungsantrag) unter Ziffer 10 „Datenschutzrechtliche Hinweise" u.a. vor, dass die in Art. 84 BayBO genannten personenbezogenen Daten des Bauherren und des Entwurfsverfassers **im Amtsblatt** veröffentlicht werden dürfen, sofern der Betroffene der Veröffentlichung nicht widersprochen hat. Der Datenschutzbeauftragte eines Landratsamtes ist nun mit der Frage an mich herangetreten, ob die personenbezogenen Daten des Bauherren/Entwurfsverfassers, sofern dieser der Veröffentlichung nach Art. 84 BayBO nicht widersprochen hat, auch dann im Amtsblatt veröffentlicht werden dürfen, wenn dieses in das Internet eingestellt wird.

Nach Art. 26 Abs. 2 der Gemeindeordnung (GO) sind Amtsblätter regelmäßig erscheinende **Druckwerke**. Aus dem datenschutzrechtlichen Hinweis in dem o.g. amtlichen Bauantrags-Vordruck, dass die genannten personenbezogenen Daten im Amtsblatt veröffentlicht werden dürfen, muss der Bauherr/ Entwurfsverfasser daher nicht mit einer Veröffentlichung seiner personenbezogenen Daten im Internet rechnen. Voraussetzung für ein wirksames Ausüben des Widerspruchsrechts nach Art. 84 BayBO ist aber die Kenntnis des Betroffenen darüber, welche Folge es hat, wenn er nicht widerspricht. Er muss deshalb auf die Möglichkeit einer Veröffentlichung seiner personenbezogenen Daten (auch) im Internet, wenn er von seinem Widerspruchsrecht keinen Gebrauch macht, ausdrücklich hingewiesen werden. Das Innenministerium, an das ich mich gewandt habe, teilt meine Auffassung und hat mir zugesichert, den Hinweis auf das Widerspruchsrecht in dem o.g. Vordruck im Zuge der nächsten Änderung der Vordrucke entsprechend zu ergänzen.

11.6 Inanspruchnahme von Inkassounternehmen im Verwaltungsvollstreckungsverfahren

Eine Stadt hat sich an mich mit der Frage gewandt, ob datenschutzrechtliche Bedenken dagegen bestehen, private Inkassounternehmen bei der Durchsetzung von Forderungen der Kommune einzuschalten. Nach Mitteilung der Stadt sollte sich das Inkassounternehmen nur mit den hartnäckigen Schuldnern „beschäftigen", die auf keine der städtischen Maßnahmen (z.B. durch den Außendienst) reagiert haben. Mit dem Mahnverfahren sollte das Inkassounternehmen nicht beauftragt werden. Alle Fälle, die an das Inkassounternehmen abgegeben werden sollen, seien von der Kasse gemahnt worden, hätten von der Vollstreckungsstelle bei öffentlich-rechtlichen Forderungen eine Vollstreckungsankündigung bzw. bei privatrechtlichen Forderungen eine verschärfte Zahlungsaufforderung erhalten und seien zum großen Teil auch vom Außendienst zur Zahlung aufgefordert worden. Bei diesem Sachverhalt bin ich davon ausgegangen, dass das Inkassounternehmen mit der Forderungsbeitreibung betraut werden sollte.

Zusammengefasst vertrete ich dazu folgende Auffassung:

Die Beitreibung von Klinikrechnungen durch Inkassounternehmen ist nach Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz grundsätzlich zulässig, bei der Datenübermittlung ist aber das Arztgeheimnis soweit wie möglich zu wahren.

Ob die Beauftragung von Inkassounternehmen mit dem Beitreiben von Forderungen aus dem Sozialbereich zulässig ist, unterliegt erheblichen Zweifeln.

Sollen für die Beitreibung sonstiger Forderungen Inkassounternehmen mit der Verarbeitung sonstiger sensibler Daten beauftragt werden, so sollte hiervon aus Gründen des Datenschutzes abgesehen werden.

Im Einzelnen:

Zunächst ist zu prüfen, inwieweit bereichsspezifische gesetzliche Regelungen zu berücksichtigen sind. So stellt sich z.B. bei der Einschaltung eines externen Inkassounternehmens durch einen (hier kommunalen) Krankenhausträger die Frage nach der Reichweite der Befugnis aus Art. 27 Abs. 5 Satz 1 Bayerisches Krankenhausgesetz. Nach dieser Bestimmung ist die Übermittlung von Patientendaten an Dritte unter anderem zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses zulässig. Diese Vorschrift kann vom Grundsatz her die Weitergabe von Daten an ein Inkassounternehmen zum Zwecke des vorgerichtlichen Forderungseinzugs rechtfertigen. Allerdings müsste der Krankenhausträger unter Beachtung des Verhältnismäßigkeitsgrundsatzes so schonend wie möglich vorgehen, um das Arztgeheimnis möglichst zu wahren. Zu den Konsequenzen, die insbesondere daraus gezogen werden müssen, verweise ich auf meinen Beitrag Nr. 3.4.1.3 im 17. Tätigkeitsbericht 1996.

Zur Beitreibung von Forderungen der Sozialhilfeverwaltung habe ich die Stadt darauf hingewiesen, dass die in ihrem Schreiben genannte Vorschrift des § 80 SGB X hier nicht einschlägig ist. Eine Verarbeitung oder Nutzung von Sozialdaten im Auftrag liegt in diesem Sinne unter anderem nur dann vor, wenn sie **Kerninhalt** und nicht lediglich unvermeidbares Nebenprodukt der Auftragserteilung ist. Ge-

genstand des von der Stadt angedachten Outsourcings war jedoch vielmehr eine Beitreibung titulierter Forderungen (unter anderem) der Sozialhilfeverwaltung.

Aber auch die Voraussetzungen des § 69 Abs. 1 Nr. 1 SGB X, der hier als einzige Datenübermittlungsbefugnis in Betracht kommen könnte, habe ich nicht für erfüllt angesehen. Dies lag nicht etwa nur daran, dass die städtische Vollstreckungsstelle nach dem Schreiben der anfragenden Stadt und den beigefügten Anlagen keine Ausführungen dazu machte, inwieweit die Einschaltung von Inkassobüros und - damit verbunden - auch die Datenübermittlungen an diese Stellen i.S.d. SGB-Vorschrift als „erforderlich“ bzw. angemessen zu beurteilen wären (vgl. hierzu unter anderem die Voraussetzungen nach § 80 Abs. 5 SGB X).

Insbesondere habe ich Zweifel bezüglich der Zulässigkeit einer Datenweitergabe an Inkassobüros zur Beitreibung titulierter Forderungen der (Sozialhilfe-) Verwaltung, weil dies wohl eine **rechtlich unzulässige Funktionsübertragung** darstellen dürfte. Die Art. 18 ff. des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes (VwZVG) ermöglichen der Behörde die Vollstreckung ihrer Verwaltungsakte (§ 66 Abs. 3 SGB X). Daneben kann gemäß § 66 Abs. 4 SGB X aus einem Verwaltungsakt auch die Zwangsvollstreckung in entsprechender Anwendung der ZPO stattfinden. Angesichts der genannten Vorschriften ist mir nicht ersichtlich, dass die Beitreibung von Forderungen darüber hinaus im Wege des „Outsourcings“ erfolgen dürfte. Diese Frage ist zwar wegen der Prüfung, ob Datenübermittlungen an Inkassobüros überhaupt erforderlich sein können, auch datenschutzrechtlich von Relevanz, sie ist jedoch **primär aus fachlicher Sicht** und insoweit nicht vom Bayerischen Landesbeauftragten für den Datenschutz zu entscheiden.

Diese Aussage zur rechtlichen Beurteilung der Einschaltung von Inkassobüros zur Beitreibung titulierter Forderungen der Sozialhilfeverwaltung als eine wohl rechtlich unzulässige Funktionsübertragung gilt in gleicher Weise auch für Forderungen aus anderen Verwaltungsbereichen.

Auch soweit an eine Einschaltung von Inkassobüros bei Tätigkeiten gedacht wird, die keine rechtlich unzulässige Funktionsübertragung, sondern eine Datenverarbeitung im Auftrag (Art. 6 BayDSG) darstellen (wie dies z.B. bei der Vergabe steuerlicher **Hilfs**tätigkeiten grundsätzlich als zulässig angesehen wird), ist zu berücksichtigen, dass hier in aller Regel sensible Bereiche betroffen sind und dem Inkassounternehmen besonders schutzwürdige personenbezogene Daten des Schuldners (wie z.B. die Tatsache der Zahlungsunfähigkeit) bekannt werden können und ein Outsourcing deshalb auch insoweit unterbleiben sollte.

Zu privatrechtlichen Forderungen teile ich die Auffassung des sächsischen Datenschutzbeauftragten in Ziffer 5.5.9 seines 7. Tätigkeitsberichts, dass die Kommunen ihre privatrechtlichen Forderungen selbst wirkungsvoll außergerichtlich geltend machen können und die Schuldnerdaten deshalb nicht an ein Inkassounternehmen weitergegeben werden sollten.

11.7 Erhebung, Verarbeitung und Nutzung von Wahlhelferdaten

Eine Stadt hat sich mit der Frage an mich gewandt, unter welchen Voraussetzungen die Erhebung, Verarbeitung und Nutzung von Daten von Wahlberechtigten zum Zwecke der Besetzung von Wahlvorständen bei Bundestags-, Landtags-, Europa- und Kommunalwahlen zulässig ist (vgl. hierzu auch 20. Tätigkeitsbericht 2002, Ziffer 9.1). Die Rechtslage stellt sich zusammengefasst wie folgt dar:

Bundes- und Landeswahlgesetz berechtigen zur Verarbeitung von Daten Wahlberechtigter zum Zweck der Besetzung von Wahlvorständen. Gegen die Verarbeitung der Daten für künftige Wahlen haben die Betroffenen ein Widerspruchsrecht.

Öffentliche Stellen des Bundes und der Länder sind nach den genannten Gesetzen verpflichtet, den Gemeinden auf Ersuchen zur Durchführung von Bundes- und Landtagswahlen Daten ihrer Bediensteten zu benennen.

Für Kommunalwahlen ergibt sich das Recht zur Verarbeitung von Wahlberechtigten- und von Bedienstetendaten bis zu einer Regelung in den Kommunalwahlgesetzen aus dem Bayerischen Datenschutzgesetz. Es erscheint angemessen den Betroffenen auch insofern ein entsprechendes Widerspruchsrecht einzuräumen.

Der Gesetzgeber hat in § 9 Abs. 4 Bundeswahlgesetz (BWG) und Art. 7 Abs. 4 Landeswahlgesetz (LWG) bereichsspezifische Vorschriften für die Erhebung, Verarbeitung und Nutzung von Daten von Wahlberechtigten zum Zwecke der Besetzung von Wahlvorständen bei Bundes- und Landtagswahlen erlassen. Über § 4 Europawahlgesetz (EuWG) gilt § 9 Abs. 4 BWG auch für die Europawahlen.

Gemäß § 9 Abs. 4 Satz 1 BWG bzw. Art. 7 Abs. 4 Satz 1 LWG sind die Gemeindebehörden befugt, personenbezogene Daten von Wahlberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen zu erheben, zu verarbeiten und zu nutzen. Die zu diesem Zweck erhobenen Daten dürfen auch für künftige Wahlen verarbeitet werden, sofern der Betroffene nicht widersprochen hat (§ 9 Abs. 4 Satz 2 BWG, Art. 7 Abs. 4 Satz 2 LWG). Der Betroffene ist

über das Widerspruchsrecht zu unterrichten (§ 9 Abs. 4 Satz 3 BWG, Art. 7 Abs. 4 Satz 3 LWG). Im Einzelnen dürfen folgende Daten erhoben, verarbeitet und genutzt werden: Name, Vorname, akademische Grade, Geburtsdatum, Anschriften, Telefonnummern, Zahl der Berufungen zu einem Mitglied der Wahlvorstände und die dabei ausgeübte Funktion (§ 9 Abs. 4 Satz 4 BWG, Art. 7 Abs. 4 Satz 4 LWG).

Nach § 9 Abs. 5 BWG sind die Behörden des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, der Länder, der Gemeinden, der Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts verpflichtet, auf Ersuchen der Gemeindebehörden zur Sicherstellung der Wahldurchführung von Bundestagswahlen aus dem Kreis ihrer Bediensteten Personen, die im Gebiet der ersuchenden Gemeinde wohnen, zum Zweck der Berufung als Mitglieder der Wahlvorstände zu benennen. Nach Art. 7 Abs. 5 LWG gilt diese Verpflichtung auch für Behörden des Freistaates Bayern, der Gemeinden, der Landkreise und der Bezirke sowie der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts im Hinblick auf Landtagswahlen. Es dürfen Name, Vorname, akademische Grade, Geburtsdatum, Anschriften und Telefonnummern des Bediensteten übermittelt werden (§ 9 Abs. 5 Satz 1 BWG, Art. 7 Abs. 5 Satz 1 LWG). Die ersuchte Stelle hat die Betroffenen über die übermittelten Daten und den Empfänger zu benachrichtigen (§ 9 Abs. 5 Satz 2 BWG, Art. 7 Abs. 5 Satz 2 LWG).

Rechtsgrundlage für die Weitergabe von Beschäftigtendaten zum Zwecke der Bildung von Wahlvorständen bei Kommunalwahlen ist Art. 17 Abs. 2 Nr. 12 Bayerisches Datenschutzgesetz (BayDSG). Danach dürfen die in dieser Vorschrift aufgeführten und an sich für Zwecke der Personalverwaltung und Personalwirtschaft erhobenen Beschäftigtendaten auch für die Durchführung von Kommunalwahlen weitergegeben werden. Diese Bestimmung geht als Spezialregelung den restriktiven Verarbeitungsbestimmungen des Personalaktenrechts vor. Ein Widerspruchsrecht des Betroffenen sieht Art. 17 BayDSG nicht vor. Da die Kommunen bis zur Schaffung einer entsprechenden Regelung im Kommunalwahlrecht wohl kaum getrennte Wahlhelferdateien für Bundes-, Landes- und Europawahlen einerseits und Wahlhelferdateien für Kommunalwahlen andererseits führen werden, habe ich angeregt, den Betroffenen auch bei Kommunalwahlen ein Widerspruchsrecht einzuräumen. Im übrigen ist ein derartiges Widerspruchsrecht auch aus Datenschutzgründen angemessen. Es wäre nicht einzusehen, warum den Betroffenen ein Widerspruchsrecht gegen die Speicherung ihrer Daten bei Bundes und Landtagswahlen eingeräumt wird, bei Kommunalwahlen dagegen nicht (vgl. auch Wilde/Ehmann/Niese/Knoblauch, Kommentar zum BayDSG, Art. 17, Rdnrn. 45 - 45 c).

11.8 Akteneinsicht in Bauakten

Ein Bürger hat sich bei mir darüber beschwert, dass eine Stadt Unterlagen aus den Bauakten seines in seinem Alleineigentum stehenden Anwesens an eine Rechtsanwaltskanzlei übersandt hatte, die seine Ehefrau in dem aktuell anhängigen Scheidungsverfahren vertrat. Die von mir zur Stellungnahme aufgeforderte Stadt teilte mir mit, dass die Ehefrau glaubhaft erklärt habe, dass sie Informationen aus der Bauakte, z.B. über die Größe der bisher gemeinsam bewohnten Wohnung, zur Geltendmachung ihrer rechtlichen Interessen benötige. Dies sei als Antrag auf Akteneinsicht gemäß Art. 29 Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) gewertet worden. Die Akteneinsicht sei in der Form gewährt worden, dass die begehrten Informationen an die Rechtsanwaltskanzlei weitergeleitet worden seien.

Ich habe die Akteneinsicht als datenschutzrechtlich unzulässig angesehen, da dem Interesse der Ehefrau die datenschutzwürdigen Interessen des Ehemannes gegenüberstanden. Die Ehefrau hätte im Rahmen des anstehenden Scheidungsverfahrens die Akteneinsicht zivilrechtlich erstreiten müssen.

Im Einzelnen:

Die Gewährung der Akteneinsicht an die Ehefrau und die Übermittlung der Unterlagen aus den Bauakten des Anwesen an die Rechtsanwaltskanzlei stellte eine Übermittlung personenbezogener Daten an eine nicht-öffentliche Stelle dar (Art. 4 Abs. 6 Satz 1 Nr. 3 Bayerisches Datenschutzgesetz - BayDSG). Nach Art. 15 Abs. 1 BayDSG ist die Übermittlung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Einwilligung des Betroffenen in die Datenübermittlung lag nicht vor. Zu den in Frage kommenden Rechtsgrundlagen ist Folgendes zu sagen:

Die Akteneinsicht in einem laufenden Verwaltungsverfahren ist in Art. 29 Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) geregelt. Danach hat die Behörde den Beteiligten Einsicht in die einzelnen Teile der das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (Art. 29 Abs. 1 Satz 1 BayVwVfG). Ein Rechtsanspruch auf Akteneinsicht außerhalb eines Verwaltungsverfahrens besteht grundsätzlich nicht, kann jedoch im Rahmen einer Ermessensausübung in Betracht kommen, wenn der Anspruchsteller ein

berechtigtes Interesse hieran geltend macht (vgl. BayVGH, Urteil vom 17.12.1998, BayVBl. 1998, 693 ff. m.w.N.).

Da die Ehefrau nicht Beteiligte eines laufenden Verwaltungsverfahrens war, bestand kein Anspruch auf Akteneinsicht gem. Art. 29 BayVwVfG. Auch im Rahmen einer Ermessensentscheidung durfte die Stadt die Akteneinsicht nicht gewähren, wie sich aus Folgendem ergibt:

Zur Gewährung von Akteneinsicht im Rahmen einer Ermessensentscheidung führt der BayVGH im o.b. Urteil aus, dass diese so zu treffen ist, dass unter Berücksichtigung des Grundprinzips des rechtsstaatlichen, fairen Verfahrens eine beiderseits sachgerechte Interessenwahrung möglich ist. Außerdem müsse die Kenntnis des Akteninhalts Voraussetzung für eine wirksame Rechtsverfolgung sein. Diese Grundsätze entsprechen denen einer Prüfung nach Art. 19 Abs. 1 Nr. 2 BayDSG.

Nach Art. 19 Abs. 1 Nr. 2 BayDSG ist eine Datenübermittlung 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 ist jedes nach vernünftigen Erwägungen unter Berücksichtigung der Besonderheiten des Falles anzuerkennendes, der Rechtsordnung nicht widersprechendes Interesse. Die Schutzwürdigkeit der Interessen des Betroffenen an dem Ausschluss der Datenübermittlung beurteilt sich maßgeblich anhand der Sensibilität der Daten. Erforderlich ist eine Abwägung unter Einbeziehung sämtlicher Umstände des Einzelfalles (vgl. Wilde/Ehmann/Niese/ Knoblauch, Bayerisches Datenschutzgesetz, Art. 19, Rdnr. 14 ff).

Ein berechtigtes Interesse der Ehefrau, die Daten zur Benennung der Größe der Wohnung im Rahmen des Scheidungsverfahrens zu erhalten, konnte zwar bejaht werden. Allerdings stand diesem das grundsätzlich schutzwürdige Interesse des Ehemannes an der Geheimhaltung seiner Daten, die die Bauakte des in seinem Alleineigentum stehenden Anwesens enthielt, gegenüber. Die Ehefrau hätte die Erlangung der für das Scheidungsverfahren erforderlichen Auskünfte mit der Durchsetzung von Auskunftsansprüchen nach zivilrechtlichen Anspruchsgrundlagen anstreben müssen. Die Entscheidungserheblichkeit der zu offenbarenden Auskunft für den zugrunde liegenden Rechtsstreit und gegebenenfalls entgegenstehende Rechte Dritter hätten dann von der in der Sache zur Entscheidung berufenen Gerichtsbarkeit - hier: den Zivilgerichten - beurteilt werden können. Im Ergebnis konnte daher von einem überwiegenden schutzwürdigen Interesse des Ehemannes an dem Ausschluss der Datenübermittlung ausgegangen werden.

11.9 Einrichtung einer dateigestützten Passabgleichstelle

Der Bayerische Landtag hat die Staatsregierung mit Beschluss vom 25.06.2003 (LT-Drs. 14/12816) aufgefordert, über die rechtlichen und organisatorischen Möglichkeiten, eine dateigestützte Passabgleichstelle einzurichten, schriftlich zu berichten und mir den Bericht zur Stellungnahme zuzuleiten.

Mit der Einrichtung einer dateigestützten Passabgleichstelle soll die Möglichkeit geschaffen werden, die bei verschiedenen Behörden im Bundesgebiet vorhandenen herrenlosen Ausweisdokumente ausländischer Staatsangehöriger den in Deutschland lebenden Ausländern mit ungeklärter Identität zuordnen zu können. Dazu sollen bundesweit die nicht zuzuordnenden Personaldokumente (Lichtbilder) digital erfasst und über Landeszentralstellen in einen Zentralserver eingestellt werden, der bei einer Landesbehörde angesiedelt werden soll. Die Landeszentralstellen sollen täglich Kopien des aktualisierten bundesweiten Bestandes des Zentralrechners für einen automatisierten Bild-zu-Bild-Abgleich mit den Lichtbildern passloser Personen erhalten, die zurückgeführt werden sollen.

Ich habe mich aus datenschutzrechtlicher Sicht zu dem Vorhaben wie folgt geäußert:

Mit einer dateigestützten Passabgleichstelle würde in das informationelle Selbstbestimmungsrecht der betroffenen Ausländer dadurch eingegriffen, dass Bilddaten aus Personaldokumenten in einer zentralen Datei gespeichert und mit Lichtbildern passloser Personen verglichen werden. Hierfür wäre eine bereichsspezifische Befugnisnorm erforderlich. Der zunächst dafür von einer Bund-Länder-Arbeitsgruppe der Innenministerkonferenz vorgesehene § 63 Abs. 2 Ausländergesetz reicht hierfür nicht aus, weil es sich bei dieser Bestimmung um eine reine Verfahrensvorschrift handelt, mit der nur Aufgaben, die bereits in den Zuständigkeitsbereich der Ausländerbehörden fallen, auf bestimmte einzelne Behörden übertragen werden können, nicht jedoch Befugnisse zur Einrichtung besonderer Verfahren begründet werden.

Mit anderen Datenschutzbeauftragten bin ich deshalb der Meinung, dass für das vorgesehene Verfahren eine besondere Befugnisnorm, wohl im Bundesrecht, geschaffen werden müsste. Die von der Innenministerkonferenz eingesetzten Arbeitskreise I und II teilen diese Auffassung und haben der Innenministerkonferenz empfohlen, für die Errichtung der Passabgleichstelle eine gesetzliche Grundlage zu schaffen. Die Innenministerkonferenz hat daraufhin mit Beschluss vom 15.05.2003 den Bundesminister des Innern gebeten, die notwendigen bereichsspezifischen bundesgesetzlichen Regelungen vorzubereiten.

In der Sache hätte ich, vorbehaltlich der primären Zuständigkeit des Bundesbeauftragten für den Datenschutz für die Beurteilung von Bundesgesetzen in datenschutzrechtlicher Hinsicht, gegen die Einrichtung einer dateigestützten Passabgleichstelle auf einer gesetzlichen Grundlage, in der die Datenerhebung, -verarbeitung und -nutzung im Rahmen des Erforderlichen bereichsspezifisch geregelt wird, keine datenschutzrechtlichen Einwände. Nach der Rechtsprechung des Bundesverfassungsgerichts sind Eingriffe in das Recht auf informationelle Selbstbestimmung auf der Grundlage eines normenklaren Gesetzes im überwiegenden Interesse der Allgemeinheit nach Abwägung mit der Tiefe des Eingriffs zulässig. Das überwiegende Interesse der Allgemeinheit liegt darin, dass die Vielzahl der herrenlosen Pässe den Inhabern zugeordnet werden können, damit die ungeklärten Identitäten festgestellt und gegebenenfalls auch Ausreiseverpflichtungen durchgesetzt werden können. Demgegenüber schätze ich den Eingriff in das Recht auf informationelle Selbstbestimmung als weniger gewichtig ein, da mit der Fertigung des Lichtbilds, dessen Aufnahme in die Datei und dem Abgleich lediglich rechtliche Verpflichtungen des Betroffenen realisiert werden sollen. Auch gegen die Nutzung der Datei zu bestimmten polizeilichen Zwecken erhebe ich bei entsprechender gesetzlicher Absicherung keine grundsätzlichen Bedenken, da diese Datei zur Abklärung der Personenidentität im Zusammenhang mit Straftaten genutzt werden kann. Auch hieran besteht ein überwiegendes öffentliches Interesse. Für eine Beurteilung im Einzelnen bleibt ein Gesetzentwurf abzuwarten.

11.10 Aufzeichnung von Telefongesprächen durch einen städtischen Verkehrsbetrieb

Im Berichtszeitraum bin ich von der Presse darüber informiert worden, dass ein städtischer Verkehrsbetrieb alle eingegangenen Telefongespräche, z.B. von Personen die Auskünfte über den Fahrplan, Haltestellen etc. wünschten, ohne Kenntnis der Betroffenen aufgezeichnet hat. Die datenschutzrechtliche Überprüfung hat ergeben, dass der Verkehrsbetrieb alle auf einer Servicenummer und einer Amtsnummer eingegangenen internen und externen Gespräche auf einem Voice Recorder gespeichert hat. Ziel der Aufzeichnung war nach den Angaben des Unternehmens eine Unterstützung des Störungs- und Sicherheitsmanagements im öffentlichen Verkehrsbereich (u.a. Gefahrenabwehr und Beweissicherung). Aus datenschutzrechtlicher Sicht habe ich die Aufzeichnung mit Ausnahme von Notrufen und Störungsmeldungen für unzulässig erachtet.

Im Einzelnen:

Die Aufzeichnung eingehender Anrufe erfüllt den Straftatbestand des § 201 Abs. 1 Nr. 1 StGB, da sie das nicht öffentlich gesprochene Wort der Anrufer erfasst. Darunter fällt jedes nicht an die Allgemeinheit gerichtete, nicht über einen durch persönliche oder sachliche Beziehungen abgegrenzten Personenkreis hinaus ohne weiteres wahrnehmbare gesprochene Wort.

Die Aufnahme der Gespräche erfolgt unbefugt, soweit keine Rechtfertigungsgründe eingreifen. Eine Rechtfertigung der Aufzeichnungen nach § 34 StGB kann im Einzelfall zur Abwehr einer gegenwärtigen Gefahr für eines der in dieser Vorschrift aufgezählten Rechtsgüter in Betracht kommen, wenn Notrufe bzw. Anrufe, die der Mitteilung akuter und gefährlicher Störungen dienen, eingehen.

Mangels einer konkreten gegenwärtigen Gefahr kann aber nicht die Aufzeichnung sämtlicher eingehender Anrufe (im vorliegenden Fall auf der Amts- oder Service-Rufnummer) auf § 34 StGB gestützt werden. Dies wäre nur in ganz besonderen Ausnahmefällen aufgrund akuter Bedrohungs- oder Gefährdungssituationen möglich.

Auch durch einen Hinweis auf die Aufzeichnung lassen sich die Datenschutzbedenken gegen eine Aufzeichnung sämtlicher Anrufe nicht ausräumen. Eine informierte Einwilligung im Sinne des Bayerischen Datenschutzgesetzes würde voraussetzen, dass die Einwilligung umfassend erteilt wird. Dazu wäre eine entsprechende vorherige Aufklärung des Einwilligenden notwendig. Die Anrufer müssten dabei vor Abgabe der Einwilligung auch darüber aufgeklärt werden, für welchen Zeitraum eine Speicherung erfolgt und zu welchen Zwecken dies geschieht. Eine informierte und umfassende Einwilligung setzt außerdem voraus, dass der Anrufer eine „echte Ausweichmöglichkeit“ hat, um die begehrten Auskünfte zu erhalten (also dass er z.B. auch auf einer anderen Rufnummer, bei der keine Aufzeichnungen stattfinden, anrufen kann und Auskunft erhält).

Im Ergebnis habe ich danach gegen die Aufzeichnungen von externen Telefongesprächen aus datenschutzrechtlicher Sicht nur insoweit keine Bedenken, als folgende Voraussetzungen gegeben sind:

- Eine Aufzeichnung aller externen Telefonate ist nur auf einer gesonderten Rufnummer für Notrufe oder Störungsmeldungen zulässig. Der Anrufer ist auf die Aufzeichnung und die Speicherung des Gesprächs, z.B. per Bandansage, hinzuweisen.

- Eine Aufzeichnung auf sogenannten Service-Nummern (z.B. Amtsnummer, Rufnummern für Fahrplan- und Tarifauskünfte u.ä.) ist grundsätzlich unzulässig. Nur bei Vorliegen eines Notfalles (z.B. Unfallmeldung, Bombendrohung) wäre eine Aufzeichnung, die durch den Sachbearbeiter manuell per Knopfdruck auszulösen wäre, zulässig.

- Die Aufzeichnungen sind gegen unbefugte Zugriffe zu sichern. Sie dürfen nur zur Gefahrenabwehr sowie zur Beweismittelsicherung und Fahndung durch die Polizei ausgewertet werden.

Im vorliegenden Fall hat mir der städtische Verkehrsbetrieb, mit dem ich die Sach- und Rechtslage erörtert habe, mitgeteilt, dass er eine Aufzeichnung der externen Telefongespräche auf der sogenannten Service- und der Amtsnummer grundsätzlich nicht mehr vornimmt. Nur für Notfälle könne eine Aufzeichnung durch den Sachbearbeiter manuell per Knopfdruck durchgeführt werden.

11.11 Datenschutz bei Bürgerbegehren

Bürger haben sich bei mir darüber beschwert, dass der erste Bürgermeister ihrer Gemeinde bei der Behandlung eines Bürgerbegehrens in öffentlicher Gemeinderatssitzung darauf hingewiesen hat, dass „von 58 der über 18-jährigen Bürger, die in einer bestimmten Straße wohnen, nur 12 das Bürgerbegehren unterschrieben“ hätten.

Diesen erneuten Verstoß gegen den Datenschutz bei der Auswertung von Unterschriftenlisten eines Bürgerbegehrens durch eine Gemeinde nehme ich zum Anlass, auf meine Ausführungen dazu im 19. Tätigkeitsbericht 2000 Nr. 8.6, 18. Tätigkeitsbericht 1998 Nr. 8.4.2 und 17. Tätigkeitsbericht 1996 Nr. 8.4.2 hinzuweisen. Gemeinden und Landkreise haben danach bei der Auswertung der für ein Bürgerbegehren abgegebenen Unterschriftenlisten den Grundsatz der Zweckbindung (Art. 17 Abs. 1 Nr. 2 BayDSG) zu beachten. Die Unterschriften dürfen nur hinsichtlich der Frage ausgewertet werden, ob das Bürgerbegehren von einer ausreichenden Zahl antragsberechtigter Gemeinde- bzw. Kreisbürger (Art. 18 a Abs. 6 GO, Art. 12 a Abs. 6 LKrO) unterschrieben worden ist. Auch das Innenministerium hat wiederholt, z.B. durch Rundschreiben, auf die Notwendigkeit der Einhaltung der Datenschutzvorschriften bei der Behandlung von Bürgerbegehren hingewiesen.

Die Eintragungslisten eines Bürgerbegehrens sind nicht dazu da, das Beteiligungsverhalten bestimmter Bevölkerungsgruppen auszuwerten und zu bewerten, sondern ausschließlich dazu, das notwendige Quorum für die Zulässigkeit des Bürgerbegehrens festzustellen.

11.12 Veröffentlichung personenbezogener Daten in einer Ortsteilversammlung

Durch die Eingabe eines Bürgers ist mir folgender Sachverhalt bekannt geworden:

Eine Gemeinde hatte alle Grundstückseigentümer eines Ortsteils schriftlich aufgefordert, innerhalb von vier Wochen eine Erklärung über die fachgerechte Entsorgung des beim Betrieb ihrer Kleinkläranlagen angefallenen Fäkalschlamms abzugeben. In einer Ortsteilversammlung zwei Monate später las der erste Bürgermeister der Gemeinde die Namen derjenigen Grundstückseigentümer öffentlich vor, die bis dato noch keine Erklärung zur Fäkalschlammentsorgung bei der Gemeinde abgegeben hatten. Nach Angabe der Gemeinde wollte der erste Bürgermeister die Gelegenheit wahrnehmen, die Betroffenen an die Abgabe der Erklärung zu erinnern.

Die öffentliche Bekanntgabe der Namen der Personen, die bis zur Ortsteilversammlung keine Erklärung zur Fäkalschlammentsorgung gegenüber der Gemeinde abgegeben hatten, stellte eine Übermittlung personenbezogener Daten an die Allgemeinheit dar, für die es keine Rechtsgrundlage gibt. Es wäre ausreichend und auch zulässig gewesen, die betroffenen Grundstückseigentümer allgemein und ohne Nennung ihres Namens darauf hinzuweisen, dass die Frist zur Abgabe der Erklärung bereits verstrichen war.

Dadurch, dass die Gemeinde die Betroffenen in Anwesenheit von Dritten namentlich daran erinnerte, dass die Frist bereits abgelaufen war und sie aufforderte, die fehlenden Erklärungen nachzuholen, wurden sie als säumig bzw. nachlässig dargestellt. Die Betroffenen wurden durch diese Datenübermittlung an die Öffentlichkeit quasi an den Pranger gestellt. Dies stellte einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar, den ich förmlich beanstandet habe.

11.13 Übermittlung personenbezogener Daten bei der Durchführung des Vormerk- und Belegungsverfahrens im Vollzug des Wohnungsbindungsrechts

Die behördliche Datenschutzbeauftragte eines Landratsamtes hat mich um eine datenschutzrechtliche Bewertung der folgenden Sachverhalte in der Vorgehensweise des Landratsamtes bei der Durchführung

des Vormerk- und Belegungsverfahrens im Vollzug des Wohnungsbindungsrechts gebeten.

1. Einreichung des Antrags auf Vormerkung bei den Gemeinden

Nach Mitteilung des Landratsamtes wird der Antrag auf Vormerkung für eine öffentlich geförderte Wohnung vom Wohnungssuchenden mit allen erforderlichen Unterlagen (z.B. Einkommensnachweise, Atteste, Schwerbehindertenausweis etc.) grundsätzlich zunächst beim Einwohnermeldeamt der Heimatgemeinde abgegeben und von diesem bestätigt. Anschließend werden alle Unterlagen an das Landratsamt zur Prüfung des Antrags weitergeleitet.

Das Innenministerium hat mir dazu aus fachlicher Sicht mitgeteilt, für das Verfahren auf Benennung gemäß § 5 a Wohnungsbindungsgesetz (WoBindG) i.V.m. § 2 Abs. 3 Satz 2 Nr. 2 der Verordnung zur Durchführung des Wohnungsbindungsrechts (DVWoBindG) sei u.a. auch die Angabe des bisherigen Hauptwohnsitzes und der Dauer seines Bestehens im Landkreis erforderlich. Diese Voraussetzungen könnten im Einzelfall nur durch die Bestätigung des Einwohnermeldeamtes überprüft werden. Dadurch dass der Antrag unmittelbar bei der Gemeinde eingereicht wird, könne eine spätere, gesonderte Anfrage des Landratsamtes bei der zuständigen Gemeinde von vornherein vermieden werden. Antragsteller, die nicht wollen, dass ihre Heimatgemeinde über die Wohnungssuche oder über die persönlichen Verhältnisse Kenntnis erlange, könnten den Antrag auch mit einer separaten Meldebestätigung unmittelbar beim Landratsamt einreichen. Auf diese Möglichkeit würden sie ausdrücklich hingewiesen.

Ich halte das vom Landkreis praktizierte Verfahren aus datenschutzrechtlicher Sicht für zulässig, solange für den Antragsteller die Wahlmöglichkeit besteht, seine Antragsunterlagen nicht nur bei der Heimatgemeinde, sondern mit einer Meldebestätigung auch direkt beim Landratsamt einzureichen und er von diesem ausdrücklich auf diese Möglichkeit hingewiesen wird.

2. Information der Gemeinden über alle Vormerkungsentscheidungen

Das Landratsamt teilte weiter mit, dass die jeweiligen Gemeinden des Landkreises über alle sie betreffenden Vormerkungsentscheidungen informiert würden. So erhalte bei einer Antragsablehnung die Gemeinde, in der die Wohnung gesucht wurde (Zielgemeinde), ein kurzes Schreiben über die negative Entscheidung mit Angabe personenbezogener Daten des Antragstellers. Auch bei Erlass eines Vormerkbescheides erhalte die Zielgemeinde einen Abdruck des Bescheids, aus dem neben Name und Anschrift auch Dringlichkeitsmerkmale (z.B. Schwangerschaft, kinderreiche Familie u.ä.) ersichtlich seien. Zudem lasse die im Bescheid angegebene Rangstufe Rückschlüsse auf die persönlichen Verhältnisse der Betroffenen zu, da auch den Gemeinden die Rangstufenordnung bekannt sei.

Dies habe ich wie folgt beurteilt: Die Unterrichtung der Gemeinden über die (negativen und positiven) Vormerkentscheidungen stellt eine Übermittlung personenbezogener Daten an eine öffentliche Stelle dar. Mangels einer bereichsspezifischen Rechtsgrundlage im Wohnungsbindungsrecht beurteilt sich diese Datenübermittlung nach Art. 18 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG). Danach ist die Übermittlung personenbezogener Daten zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder empfangenden Stelle liegenden Aufgaben erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG zulässig wäre.

Nach Auskunft des Bayerischen Staatsministeriums des Innern ist die Übermittlung der Vormerkentscheidungen an die Gemeinden aus der Sicht des Wohnungbindungsrechts nicht erforderlich. Insbesondere die Information der Zielgemeinde über die Ablehnung von Vormerkungsanträgen unter Angabe personenbezogener Daten sei grundsätzlich nicht zur Aufgabenerfüllung der zuständigen Stelle im Rahmen des Vormerk- und Benennungsverfahrens erforderlich. In der Regel werde es genügen, die Kompetenz der Gemeinde insoweit erst unmittelbar im Vorfeld der eigentlichen Benennung in Anspruch zu nehmen, zumal häufig alte zunächst vorgemerkte Haushalte nicht mehr auch noch für eine konkret anstehende Benennung zu berücksichtigen sein würden (z.B. weil manche zwischenzeitlich bereits anderweitig eine Wohnung gefunden haben oder weil die Geltungsdauer der Vormerkung abgelaufen ist).

Nach Mitteilung des Innenministeriums erscheint auch im Hinblick auf die Möglichkeit eines gemeindlichen Benennungsvorschlags (Ziff. 7.1.3 Satz 2 VVWoBindG) eine Information der Gemeinde über alle Vormerkungs-

entscheidungen unabhängig von einer anstehenden Benennung nicht erforderlich. So sei die Gemeinde zum einen bei einem Vorschlag grundsätzlich auf Wohnungsberechtigte beschränkt (von diesen wird sie aber im Rahmen einer Abstimmung über die Auswahlentscheidung anlässlich der konkret anstehenden Benennung ohnehin ausreichend Kenntnis erlangen können); zum anderen sei auch durch einen positiven Vormerkbescheid noch nicht entschieden, ob überhaupt Gelegenheit besteht, in der Zielgemeinde eine Sozialwohnung zu beziehen.

Ich teile diese Auffassung, die dem Grundsatz Rechnung trägt, dass nur die erforderliche Datenverarbeitung zulässig ist. Auch zur Einschätzung der örtlichen Wohnraumversorgung ist eine personenbezogene Information der Gemeinden über die abgelehnten Bewerber nicht erforderlich. Für Planungszwecke der Gemeinden würden auch statistische oder aggregierte Daten ausreichen.

Ich habe das Landratsamt daher aufgefordert, künftig eine personenbezogene Unterrichtung der jeweiligen Gemeinden über die negativen oder positiven Vormerkentscheidungen zu unterlassen.

3. Benennung in Abstimmung mit der Zielgemeinde

Nach Mitteilung des Landratsamtes erfolgt die Belegung von frei werdenden Wohnungen im Einvernehmen mit der jeweiligen Zielgemeinde. Hierfür würden die dringlichsten Fälle zunächst herausgefiltert, mit der jeweiligen Gemeinde diskutiert, und danach dem Vermieter vorgeschlagen.

In Ziffer 7.1.3 VVWoBindG wird ausdrücklich darauf hingewiesen, dass sich die zuständige Stelle vor einer von ihr vorzunehmenden Benennung soweit erforderlich mit der Gemeinde abstimmen soll. Dies gilt insbesondere dann, wenn die Gemeinde kommunale Fördermittel zur Verfügung gestellt hat. Das Bayerische Staatsministerium des Innern ist darüber hinaus der Auffassung, dass auch ohne eine derartige Mitförderung eine Abstimmung mit der Gemeinde zur Erfüllung der Aufgaben der zuständigen Stelle und der Gemeinde erforderlich sein kann. So haben die Gemeinden u.a. die Aufgabe, die Belange der örtlichen Gemeinschaft bei der Versorgung mit ausreichendem und preisgünstigem Wohnraum zu wahren, was gemäß § 2 Abs. 7 DVWoBindG auch zu einer Abweichung von der bei der Benennung zu beachtenden Rangfolge der Dringlichkeit führen kann. Nach § 2 Abs. 6 Nr. 1 DVWoBindG besteht außerdem die Möglichkeit von der Rangfolge der Dringlichkeit abzuweichen, wenn dies der Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen im Sinne des Wohnraumförderungs- und Wohnungsbindungsrechts dient. Zur Realisierung dieses Ziels ist daher häufig die Einbeziehung der jeweiligen Gemeinde, die die sozialen Verhältnisse vor Ort sowie die konkreten Probleme besser kenne als die Kreisverwaltungsbehörde, erforderlich.

Die im Rahmen der Beteiligung der Gemeinden bei der Benennung von Wohnungssuchenden erfolgende Übermittlung personenbezogener Daten beurteilt sich mangels einer bereichsspezifischen Rechtsgrundlage ebenfalls nach Art. 18 Abs. 1 BayDSG. Ich teile die Auffassung des Bayerischen Staatsministeriums des Innern, wonach die Datenübermittlungen sowohl für die übermittelnde Stelle (hier: Landratsamt) als auch für die empfangende Stelle (hier: die jeweilige Zielgemeinde) zu deren Aufgabenerfüllung erforderlich sind. Die beim Landratsamt praktizierte Vorgehensweise zur Benennung in Abstimmung mit der Zielgemeinde halte ich daher aus datenschutzrechtlicher Sicht für unbedenklich.

12 Einwohnermeldewesen

12.1 Weitergabe von Melderegisterdaten an politische Parteien

Vor Wahlen erreichen mich immer wieder Anfragen und Beschwerden von Bürgern, die von politischen Parteien persönlich an sie adressierte Wahlwerbeschreiben erhalten haben. Den Bürgern war nicht bekannt, dass die Meldebehörden politischen Parteien Melderegisterauskünfte zu Wahlwerbezwecken erteilen dürfen und dass sie der Datenweitergabe durch einfache Mitteilung an ihr Meldeamt widersprechen können. Vor den letzten Landtagswahlen habe ich deshalb die Bürger durch eine Presseerklärung erneut auf ihr Widerspruchsrecht hingewiesen (vgl. dazu zuletzt 20. Tätigkeitsbericht 2002, Nr. 10.2).

Nach Art. 35 Abs. 1 Meldegesetz darf die Meldebehörde Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, den Doktorgrad und Anschriften von Gruppen von Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen maßgebend ist, es sei denn, der Bürger hat dieser Weitergabe seiner Daten widersprochen.

In § 22 Abs. 1 der am 03.04.2002 in Kraft getretenen Änderung des Melderechtsrahmengesetzes (BGBl I S. 1186) werden die Meldebehörden verpflichtet, die Wahlberechtigten bei der Anmeldung und spätestens acht 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.

Ich begrüße diese Verbesserung der Pflicht, die Bürger und Bürgerinnen auf ihr Widerspruchsrecht hinzuweisen. Mit meinen Kolleginnen und Kollegen hätte ich es jedoch vorgezogen, wenn der Gesetzgeber eine Einwilligungslösung statuiert hätte. Immerhin ist eine gewisse Verbesserung erreicht.

12.2 Übermittlung von Meldedaten sämtlicher Einwohner der Landkreisgemeinden an das Landratsamt als Katastrophenschutzbehörde

Ein Landratsamt hat mich um datenschutzrechtliche Äußerung zu Überlegungen gebeten, Meldedaten sämtlicher Einwohner der Landkreisgemeinden an das Landratsamt als Katastrophenschutzbehörde mit vierteljährlichen Aktualisierungen des Datenbestandes zu übermitteln. Das Landratsamt beabsichtigte, die Meldedaten für die Planung und Kontrolle der vollständigen Evakuierung im Katastrophenfall zu nutzen. Ich habe das Vorhaben aus den folgenden Gründen für unzulässig angesehen:

Meldebehörden sind nach Art. 1 MeldeG die Gemeinden. Durch das geplante Vorhaben würden bei der Katastrophenschutzbehörde im Landratsamt für den Bereich der übermittelten Datenbestände unzulässige Parallelmelderegister der Landkreisgemeinden entstehen.

Die vierteljährlichen Aktualisierungen wären regelmäßige Datenübermittlungen von den Meldebehörden an das Landratsamt. Nach Art. 31 Abs. 4 MeldeG sind regelmäßige Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Die Bayerische Meldedaten-Übermittlungsverordnung sieht regelmäßige Datenübermittlungen von den Meldebehörden an die Katastrophenschutzbehörden nicht vor.

Die geplanten Datenübermittlungen sind nach meinem Dafürhalten für die Erreichung der vorgesehenen Zwecke (Planung und Kontrolle der vollständigen Evakuierung im Katastrophenfall) im übrigen auch nicht geeignet bzw. nicht erforderlich:

- Für Planungszwecke sind keine personenbezogenen Angaben notwendig. Hier genügen Größenangaben (Anzahl der betroffenen Personen).

- Zum Zeitpunkt einer Evakuierung im Katastrophenfall können im Evakuierungsgebiet wohnhafte Personen abwesend oder fremde Personen anwesend sein. Auch können sich Einwohner rechtzeitig in Sicherheit gebracht haben, ohne sich bei den Katastrophenschutzkräften zu melden. Eine vollständige Räumung kann deshalb nicht zuverlässig über eine Einwohnerliste kontrolliert werden. Ein derartiges Verfahren könnte auch dazu führen, dass nach Personen gesucht wird, die sich nicht in Gefahr befinden, weil sie sich nicht in ihren bedrohten Anwesen aufhalten. Damit würden unnötig Mittel gebunden und die Rettungskräfte könnten unter Umständen selbst in Gefahr geraten. Letztlich bestünde bei dem geplanten Verfahren (vierteljährliche Datenabgleiche) immer die Gefahr, dass der Melderegisterdatenbestand im Landratsamt zum Zeitpunkt des Katastrophenfalls inaktuell ist.

12.3 Erhebung der rechtlichen Zugehörigkeit zu einer Religionsgemeinschaft

Nach § 1 Abs. 1 der Verordnung zur Durchführung des Bayerischen Gesetzes über das Meldewesen (DVMeldeG) sind für die An- und Abmeldung nach § 13 Abs. 1 und 2 MeldeG die Vordrucke nach den Mustern der Anlagen zur DVMeldeG zu verwenden. In den Vordrucken ist ein Feld „Religion“ vorgesehen, zu dem die Ausfüllanleitungen nach § 1 Abs. 3 DVMeldeG den Hinweis enthalten: „Für melderechtliche Zwecke ist lediglich die Angabe der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft erforderlich“. Aus diesem Hinweis ist für die Betroffenen nicht ersichtlich, dass nach Anlage 2 zu Blatt 1001 des Datensatzes für das Meldewesen, einheitlicher Bundes-/Länderanteil, nur die Schlüssel EV (=evangelisch), RF (=reformiert), RK (=römisch-katholisch), AK (=altkatholisch), IS (=israelitisch) und VD (=verschieden (andere Gemeinschaften, gemeinschaftslos, keine Angaben)) gespeichert werden und sie deshalb ihre Religionszugehörigkeit nur angeben müssen, wenn sie einer der in dieser Anlage genannten Glaubensgemeinschaft angehören und im übrigen die Angabe VD genügt. Ich habe daher das Bayerische Staatsministerium des Innern gebeten, die Ausfüllanleitungen zum Feld „Religion“ so zu präzisieren, dass den Betroffenen klar ist, dass sie nur die oben genannten Religionsschlüssel oder VD in dieses Feld eintragen und zu einer sonstigen bestehenden Religionszugehörigkeit (z.B. Islam) keine Angaben

machen müssen. Das Innenministerium hat mir daraufhin mitgeteilt, dass es einen Hinweis auf die abschließende Aufzählung der in Bayern zugelassenen Religionsschlüssel in der Ausfüllanleitung für sinnvoll hält und meinen Änderungswunsch zu den Angaben zur Zugehörigkeit zu einer Religionsgemeinschaft bei der nächsten Änderung der Verordnung zur Durchführung des Bayerischen Gesetzes über das Meldewesen berücksichtigen wird.

13 Ausländerwesen

13.1 Datenschutzrechtliche Kontrolle der Ausschreibungen nach Art. 96 des Schengener Durchführungsübereinkommens

Die Gemeinsame Kontrollinstanz von Schengen, die nach Art. 115 Abs. 3 des Schengener Durchführungsübereinkommens (SDÜ) auch zuständig ist für die Prüfung der Anwendungs- und Auslegungsfragen im Zusammenhang mit dem Schengener Informationssystem (SIS), beschäftigte sich im Berichtszeitraum mit der Ausschreibungspraxis nach Art. 96 SDÜ, also von Drittausländern. Ausgelöst wurde diese Initiative durch die rein zahlenmäßig sehr unterschiedliche Ausschreibungspraxis bei den Schengen-Vertragsparteien (u.a. Italien ca. 335.000 Ausschreibungen; Deutschland ca. 267.000 Ausschreibungen; Frankreich ca. 52.000 Ausschreibungen; jeweils zum 01.02.2003). Im Rahmen dieser Aktion eruierten die nationalen Kontrollinstanzen die Voraussetzungen und das Verfahren nach Art. 96 SDÜ, auch mittels datenschutzrechtlicher Kontrollen.

Zur Durchführung der datenschutzrechtlichen Kontrollen hatte sich der Bundesbeauftragte für den Datenschutz vom Bundeskriminalamt im Wege eines Zufallsgenerators eine Liste von Prüffällen erstellen lassen, in die jede 500. Ausschreibung aufgenommen wurde. Auf Bayern entfielen davon 46 Ausschreibungen von 27 Ausländerbehörden, die mir der Bundesbeauftragte für den Datenschutz übermittelt hat. Die an Hand eines bundesweit einheitlichen Fragebogens unter Mithilfe der behördlichen Datenschutzbeauftragten der betroffenen Ausländerbehörden durchgeführten Überprüfungen haben ergeben, dass die Ausschreibungen in den meisten Fällen rechtmäßig erfolgt sind. Sofern Ausschreibungen fehlerhaft oder unzulässig waren, wurden diese umgehend berichtigt bzw. gelöscht. Die bei der Überprüfung festgestellten Mängel habe ich außerdem zum Anlass genommen, beim Bayerischen Staatsministerium des Innern anzuregen, die Ausländerbehörden nochmals auf die Voraussetzungen für eine Ausschreibung nach Art. 96 SDÜ hinzuweisen.

13.2 Fragebogen zur sicherheitsrechtlichen Befragung durch die Ausländerbehörden

Am 01.01.2002 ist das Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) in Kraft getreten (BGBl I 2002, S. 361 ff.). Vor dem Hintergrund der Ereignisse vom 11. September 2001 hat darin auch das Ausländerrecht zahlreiche Änderungen erfahren. Dazu zählen u.a. folgende, auf die ich hier eingehe, da sie Rückwirkungen auf Datenerhebungen haben:

In § 8 Abs. 1 Ausländergesetz (AuslG) wurde unter der neuen Nr. 5 ein besonderer Versagungsgrund aufgenommen. Danach ist eine Aufenthaltsgenehmigung auch bei Vorliegen der Voraussetzungen eines Anspruchs zwingend zu versagen, wenn der Ausländer die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährdet oder sich bei der Verfolgung politischer Ziele an Gewalttätigkeiten beteiligt oder öffentlich zur Gewaltanwendung aufruft oder mit Gewaltanwendung droht oder wenn Tatsachen belegen, dass er einer Vereinigung angehört, die den internationalen Terrorismus unterstützt oder er eine derartige Vereinigung unterstützt.

Nach § 46 Nr. 1 AuslG kann ein Ausländer auch ausgewiesen werden, wenn er im Verfahren nach dem Ausländergesetz oder zur Erlangung eines Schengen-Visums falsche Angaben zum Zwecke der Erlangung einer Aufenthaltsgenehmigung oder Duldung macht oder sich trotz bestehender Rechtspflicht weigert, an Maßnahmen der für die Durchführung des Ausländergesetzes zuständigen Behörden im In- und Ausland mitzuwirken. Allerdings ist die Ausweisung nur zulässig, wenn der Ausländer vor der Befragung ausdrücklich auf die Rechtsfolgen falscher oder unrichtiger Angaben hingewiesen wurde.

Nach § 47 Abs. 2 Nr. 4 AuslG wird ein Ausländer in der Regel ausgewiesen, wenn die Voraussetzungen für einen Versagungsgrund gemäß § 8 Abs. 1 Nr. 5 AuslG vorliegen. Der ebenfalls neu in das Gesetz aufgenommene § 47 Abs. 2 Nr. 5 AuslG bestimmt, dass ein Ausländer in der Regel ausgewiesen wird, wenn er in einer Befragung, die der Klärung von Bedenken gegen die Einreise oder den weiteren Aufenthalt dient, der deutschen Auslandsvertretung oder der Ausländerbehörde gegenüber frühere Aufenthalte in Deutschland oder anderen Staaten verheimlicht oder in wesentlichen Punkten falsche oder unvollständige Angaben über Verbindungen zu Personen oder Organisationen macht, die der Unterstützung des internationalen Terrorismus verdächtig sind. Voraussetzung für die Ausweisung ist auch hier, dass der Ausländer, bevor er befragt wird, ausdrücklich auf den sicherheitsrechtlichen Zweck der Befragung und

die Rechtsfolgen falscher oder unrichtiger Angaben hingewiesen wurde.

Um einen landesweit einheitlichen Gesetzesvollzug zu gewährleisten hat das Bayerische Staatsministerium des Innern im Rahmen vorläufiger Vollzugshinweise einen Fragebogen eingeführt. Damit sollen die Ausländerbehörden in die Lage versetzt werden, durch eine standardisierte sicherheitsrechtliche Befragung vor der Erteilung einer Aufenthaltsgenehmigung die Voraussetzungen für das Vorliegen eines zwingenden Versagungsgrundes gemäß § 8 Abs. 1 Nr. 5 AuslG zu klären und eventuelle Sicherheitsbedenken bei bestimmten Personengruppen auszuräumen. So werden Personen aus Staaten befragt, bei denen mit erhöhter Wahrscheinlichkeit davon ausgegangen werden kann, dass aus ihnen mögliche Täter terroristischer Anschläge einreisen. Gleiches gilt bei Sicherheitsbedenken aufgrund ungeklärter Identität oder Staatsangehörigkeit. Ferner soll eine sicherheitsrechtliche Befragung vor der Erteilung oder Verlängerung eines Reiseausweises nach der Genfer Flüchtlingskonvention durchgeführt werden. Die Befragung dient hier sowohl der Feststellung von Ausweisungsgründen als auch der Feststellung von zwingenden Gründen der Sicherheit und Ordnung nach Art. 28 der Genfer Flüchtlingskonvention, die der Erteilung eines Reiseausweises entgegenstehen. Eine Befragung mittels Standardfragebogens kann von der Ausländerbehörde auch vor der Erteilung einer Duldung in Betracht gezogen werden, wenn sich im laufenden Verwaltungsverfahren erste Anhaltspunkte für eine entsprechende sicherheitsgefährdende Betätigung des Ausländers ergeben.

Nach der Einführung des Fragebogens habe ich dazu einige Zuschriften mit der Bitte erhalten zu prüfen, ob bei der Befragung durch die Ausländerbehörden die datenschutzrechtlichen Bestimmungen eingehalten würden. So sei unklar, ob bei der Befragung mittels des Standardfragebogens auch die Frage nach der Religionszugehörigkeit gestellt werde.

Ich habe den Petenten mitgeteilt, dass der mir vorliegende Standardfragebogen des Innenministeriums keine entsprechende Frage erhält. Nachdem auch freiwillig gemachte Angaben zur Religionszugehörigkeit im Ausländerzentralregister gespeichert werden dürfen, hat das Innenministerium auf meine Anregung hin in den vorläufigen Vollzugshinweisen zu § 3 Nr. 5 AZRG ausdrücklich darauf hingewiesen, dass die Behörden nur insoweit das Recht haben, nach der Religionszugehörigkeit zu fragen, soweit Rechte und Pflichten davon abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert (Art. 140 GG i.V.m. Art. 136 Abs. 3 Satz 2 Weimarer Verfassung).

Die Anfragen habe ich zum Anlass genommen, mich bei mehreren Ausländerbehörden zu vergewissern, dass nur der vom Staatsministerium des Innern vorgesehene Fragebogen verwendet wird und das Datum der Religionszugehörigkeit des Ausländers auch nicht auf andere Art und Weise, z.B. durch die mündliche Befragung, erhoben wird. Bei zwei weiteren Ausländerbehörden habe ich außerdem das Verfahren der sicherheitsrechtlichen Befragung vor Ort überprüft. Verstöße gegen datenschutzrechtliche Bestimmungen konnte ich nicht feststellen, insbesondere keine unzulässigen Fragen nach der Religionszugehörigkeit.

14 Umweltfragen

14.1 Veröffentlichung von Daten aus dem Bodeninformationssystem im Internet

Im September 2003 wurde ein Internetzugang für Behörden und Bürger auf das Bodeninformationssystem (BIS) eingerichtet. Das BIS wird beim Geologischen Landesamt (GLA) geführt. Es umfasst von staatlichen oder sonstigen öffentlichen Stellen erhobene Daten aus Untersuchungen über die physikalische, chemische und biologische Beschaffenheit des Bodens und des tieferen Untergrundes. Nach Nr. 7 der Verwaltungsvorschrift zum Vollzug des Bodenschutz- und Altlastenrechts in Bayern - BayBodSchVwV - vom 11.07.2000 (AllMBl S. 473) sollen auch der Öffentlichkeit aufbereitete Daten aus dem BIS zur Verfügung gestellt werden.

Die mit der Veröffentlichung im Internet zusammenhängenden datenschutzrechtlichen Fragen habe ich mit dem Staatsministerium für Umwelt, Gesundheit und Verbraucherschutz und dem GLA, die sich an mich gewandt hatten, im Februar 2003 erörtert. Dabei war insbesondere zu klären, welche Daten des BIS der Öffentlichkeit zur Verfügung gestellt werden können. Das richtet sich danach, ob es sich bei den zur Veröffentlichung vorgesehenen Daten um personenbezogene Daten handelt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse (z.B. Eigentumsverhältnisse) bestimmter oder bestimmbarer natürlicher Personen (Art. 4 Abs. 1 BayDSG).

Das BIS enthält Flächen- und Punktdaten. Flächendaten sind keine personenbezogenen Daten, so lange sie keinen grundstücksgenauen Detaillierungsgrad erreichen, der Grundstückseigentümer also nicht festgestellt werden kann. Gegen eine Veröffentlichung von Flächendaten ohne Personenbezug bestehen keine datenschutzrechtlichen Bedenken.

Punktdaten stellen eine exakte geografische Beschreibung eines Messpunktes auf der Erdoberfläche

durch Rechts- und Hochwert dar. Sie sind personenbezogene Daten im Sinne des Art. 4 Abs. 1 BayDSG, weil hier über das Liegenschaftskataster und das Grundbuch der Grundstückseigentümer bestimmbar ist. Eine Veröffentlichung von Punktdaten wäre daher ein Eingriff in das Recht auf informationelle Selbstbestimmung des betroffenen Grundstückseigentümers, soweit es sich bei diesem um eine natürliche Person handelt.

Um der Öffentlichkeit aber auch insoweit Informationen anbieten zu können, hat das GLA ein Verfahren zur Darstellung von Punktdaten im Internet-Client des BIS vorgeschlagen, gegen das aus datenschutzrechtlicher Sicht keine Bedenken bestehen. Im Internet werden danach nur solche Punktdaten veröffentlicht, die mit Hilfe eines (technischen) Verfahrens keinen Personenbezug mehr aufweisen. Dies wird dadurch erreicht, dass als kleinste Fläche des für die Objektanzeige verwendeten Symbols in der Internet-Client-Darstellung eine Fläche ausgewählt wird, bei der gewährleistet ist, dass mehrere Grundstückseigentümer Betroffene sind, so dass ein Personenbezug nicht mehr möglich ist.

Zu prüfen war auch, inwieweit Daten aus dem Projekt GEORISK (Darstellung von Hangbewegungen, Felsstürzen, Rutschungen u.ä. im bayerischen Alpenraum) der Öffentlichkeit über das Internet zugänglich gemacht werden können. Ein Personenbezug ist hier häufig dadurch gegeben, dass die Daten punktgenau sind, das heißt, einem Grundstückseigentümer zugeordnet werden können. Für die Frage der Veröffentlichung dieser Daten kommt es im Ergebnis auf eine Differenzierung zwischen offenkundigen und nicht-offenkundigen Daten an. Bei offenkundigen Daten (z.B. sichtbare Hangrutschungen auf einem bestimmten Grundstück) sind einer Veröffentlichung entgegenstehende Belange betroffener Dritter nicht ersichtlich. Eine Einstellung dieser Daten ins Internet kommt gerade auch aus Verwaltungsvereinfachungsgründen in Betracht, um einer Vielzahl von Einzelanträgen nach § 4 Umweltinformationsgesetz (UIG) zuvor zu kommen. Bei nicht-offenkundigen Daten ist nach Art. 19 Abs. 1 Nr. 2 BayDSG und § 8 UIG eine Abwägung im Einzelfall zwischen dem berechtigten Interesse der Allgemeinheit und dem schutzwürdigen Interesse des Betroffenen zu treffen. Ein überwiegendes öffentliches Interesse in eine Veröffentlichung kann bspw. dann bejaht werden, wenn eine erhöhte Gefahreneintrittswahrscheinlichkeit besteht.

15 Steuerverwaltung

15.1 Elektronische Steuererklärung ELSTER, Elektronische Lohnsteuerkarte ELSTERLohn

In meinen Tätigkeitsberichten habe ich bereits mehrfach zu den Projekten ELSTER bzw. ELSTERLohn Stellung genommen. Dies geschah sowohl aus technisch-organisatorischer Sicht (18. Tätigkeitsbericht Nr. 19.3.12) als auch aus rechtlicher Sicht (vgl. u.a. 19. Tätigkeitsbericht Nr. 11.2 und 11.3, 20. Tätigkeitsbericht Nr. 12.2). Seitdem ist die Entwicklung der Projekte weiter vorangeschritten. Zum derzeitigen Projektstand ist Folgendes zu berichten:

Bei ELSTER handelt es sich um ein Projekt der deutschen Steuerverwaltung. Auftraggeber sind die Referatsleiter Automation (Steuer) der Länder. Die Koordination des Projekts ELSTER erfolgt durch die Bund/Länder-Arbeitsgruppe StEDV unter Moderation des Bundesfinanzministeriums. Teilprojekte von ELSTER werden in verschiedenen Länderfinanzverwaltungen entwickelt. So erfolgt die Entwicklung der sog. Basisdienste in Bayern, für Arbeiten an ELSTERFormular ist die Finanzverwaltung des Landes Thüringen zuständig, für ELSTERLohn ist federführend die Finanzverwaltung des Landes Nordrhein-Westfalen verantwortlich. Die Finanzverwaltung des Landes Hessen befasst sich mit der Entwicklung eines Konzepts zur elektronischen Abfrage des Steuerkontos eines Steuerpflichtigen durch diesen selbst bzw. seinen steuerlichen Berater.

Das Staatsministerium der Finanzen hat im Zuge des weiteren Ausbaus des Projekts den Dialog mit mir gesucht. Ich konnte mehrfach an Veranstaltungen, in denen beabsichtigte Neuerungen im Projekt ELSTER vorgestellt wurden, teilnehmen und Gesichtspunkte des Datenschutzes einbringen.

Bisher wurden die Steuerdaten der ELSTER-Anwender verschlüsselt an die beiden ELSTER-Clearingstellen übermittelt und dort unmittelbar verschlüsselt an die Rechenzentren der Steuerverwaltungen der Länder weitergeleitet. Eine Clearingstelle befindet sich in Düsseldorf (zuständig für Steuerpflichtige aus Nordrhein-Westfalen), die andere in München (zuständig für Steuerpflichtige aus dem übrigen Bundesgebiet). In der neuen Konzeption der ELSTER-Clearingstellen Phase II sollen nunmehr die Steuerdaten bereits in den Clearingstellen entschlüsselt und auf technische Plausibilität geprüft werden (einschl. einer Prüfung der elektronischen Signatur). Eine Speicherung der Daten in den Clearingstellen soll aber nicht erfolgen. Im Anschluss daran sollen

die Daten verschlüsselt an die zuständigen Rechenzentren der Länder weitergeleitet werden.

Ich habe in diesem Zusammenhang eine Klärung der rechtlichen Stellung der Clearingstellen gefordert. Das Staatsministerium hat mir inzwischen mitgeteilt, dass Regelungen zur rechtlichen Stellung der Clearingstellen in eine derzeit erarbeitete Verwaltungsvereinbarung aufgenommen werden sollen.

Hinsichtlich der Einführung der elektronischen Lohnsteuerkarte (ELSTERLohn) habe ich in der Vergangenheit die Schaffung normenklarer gesetzlicher Regelungen verlangt. Mit dem Steueränderungsgesetz 2003 vom 15.12.2003 wurde in § 41 b EStG eine gesetzlichen Grundlage zur elektronischen Übermittlung der Lohnsteuerbescheinigungsdaten durch die Arbeitgeber an die Steuerverwaltung geschaffen. Das Gesetz sieht für die meisten Arbeitgeber eine Verpflichtung zur elektronischen Übermittlung ab dem Kalenderjahr 2004 vor. Für Lohnsteuerbescheinigungsdaten des Kalenderjahrs 2003 konnten Arbeitgeber auf freiwilliger Basis im Rahmen einer im Gesetz vorgesehenen Ausnahmeregelung an dem Verfahren teilnehmen. In Bayern beteiligte sich der Freistaat selbst (Bezirksfinanzdirektion München) als „Pilot"-Arbeitgeber. Die Datenübermittlung von Lohnsteuerbescheinigungsdaten von der Bezirksfinanzdirektion München an die von der Steuerverwaltung geschaffene zentrale Clearingstelle war mehrfach Gegenstand von Eingaben. Ich habe den Eingabeführern mit Hinweis auf die bestehende gesetzliche Grundlage geantwortet.

Für Zwecke der Zuordnung hat der Arbeitgeber ein Ordnungsmerkmal (sog. „eTIN") aus Namen, Vornamen und Geburtsdatum des Arbeitnehmers zu bilden. Die von mir geforderte gesetzliche Regelung - vergleichbar den zur Sozialversicherungsnummer erlassenen Bestimmungen in §§ 18 f und 18 g SGB IV - findet sich nun in § 41 b Abs. 2 EStG. Die Vorschrift sieht in Bezug auf die „eTIN" eine Zweckbindung für Zwecke des Besteuerungsverfahrens vor. Mittel- bzw. langfristig soll die „eTIN" durch ein für jeden Steuerpflichtigen vergebenes, dauerhaftes Identifikationsmerkmal ersetzt werden. Die gesetzliche Grundlage dafür wurde ebenfalls im Steueränderungsgesetz 2003 durch die Einfügung der §§ 139 a bis 139 c AO geschaffen. In diesem Zusammenhang ist auf die Gefahr hinzuweisen, dass sich solche Ordnungsmerkmale zu einem unzulässigen zentralen Personenkennzeichen entwickeln, über das die verschiedensten Datenbestände zusammengeführt werden könnten. Das wäre nach dem Volkszählungsurteil des Bundesverfassungsgerichts wegen der damit verbundenen umfassenden Registrierung des Menschen verfassungswidrig. Es muss deshalb sehr auf zuverlässige und nicht umzukehrende Zweckbindungsregeln geachtet werden. Sie sind zwingend notwendige Bestandteile bereichsspezifischer Kennzeichnungen von Personen.

Das Staatsministerium der Finanzen hat mir zugesichert, jede Suchanfrage auf einen Lohndatensatz zu protokollieren und deren Zulässigkeit stichprobenartig auszuwerten.

Das Projekt ELSTER wird von der Finanzverwaltung mit hohem Tempo weiterentwickelt. Ich werde das Projekt weiterhin aus Sicht des Datenschutzes begleiten.

15.2 Auskunftsersuchen der Finanzämter an Behörden

Immer wieder erreichen mich Anfragen (v.a. von Kommunen) betreffend die Zulässigkeit von Auskunftsersuchen der Finanzämter. Dazu ist aus datenschutzrechtlicher Sicht Folgendes zu bemerken:

Nach § 85 AO hat die Finanzbehörde die allgemeine Aufgabe, die Steuern nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben. Im Zuge dieser Aufgabe ermittelt sie den Sachverhalt von Amts wegen, wobei sie Art und Umfang der Ermittlungen selbst bestimmt. Im Rahmen des Ermittlungsverfahrens kann so auch ein Auskunftsersuchen an die Beteiligten - i.d.R. die Steuerpflichtigen -, aber auch an Dritte gerichtet werden (§ 93 AO).

Dritte i.S.d. § 93 AO können auch Behörden sein. In diesem Falle überschneidet sich die Auskunftspflicht der Behörden nach § 93 AO mit der Amtshilfepflicht der Behörden nach § 111 ff. AO.

Aufgrund § 111 Abs. 1 AO haben alle Gerichte und Behörden der Finanzverwaltung die zur Durchführung der Besteuerung erforderliche Amtshilfe zu leisten. § 112 AO definiert im Anschluss daran u.a. die Voraussetzungen einer Amtshilfe. Bei Ersuchen der genannten Art ist davon auszugehen, dass sie sich auf § 112 Abs. 1 Nr. 3 oder Nr. 4 AO stützen.

Aus datenschutzrechtlicher Sicht ist festzustellen, dass die spezialgesetzliche Regelung des § 93 AO die Frage beantwortet, ob die Übermittlung personenbezogener Daten grundsätzlich verlangt werden darf, während das Amtshilferecht die Frage beantwortet, ob die nach § 93 AO übermittelbaren Daten auch übermittelt werden müssen.

Ich vertrete daher die Auffassung, dass die weiteren in § 93 Abs. 1 AO genannten und nachfolgend näher erläuterten Voraussetzungen auch im Rahmen von konkreten Amtshilfeersuchen erfüllt sein müssen. Eine Ungleichbehandlung des Betroffenen, je nachdem ob Adressat des Auskunftsersuchens ein privater

Dritter oder eine öffentliche Stelle ist, kann vom Steuerrecht nicht gewollt sein.

Bei Auskunftsersuchen hat die Finanzbehörde bestimmte Grenzen und eine gewisse Reihenfolge der Beweiserhebung zu beachten. So normiert § 93 Abs. 1 Satz 3 AO, dass andere Personen als die Beteiligten erst dann zur Auskunft angehalten werden sollen, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. § 93 Abs. 1 Satz 3 AO ist zwar keine Muss-Vorschrift, aber auch keine bloße Kann-Vorschrift. Das „Sollen" bedeutet, dass die Finanzbehörde i.d.R. die Vorschrift beachten muss und nur in begründeten, atypischen Ausnahmefällen davon abweichen darf.

Vor einem Auskunftsersuchen - z.B. an eine Kommune - hat die Finanzbehörde daher darzulegen, dass der Vorschrift des § 93 Abs. 1 Satz 3 AO Genüge getan worden ist. Ist dies der Fall, könnte die Gemeinde eine Auskunftserteilung nur vermeiden, wenn einer der Hinderungsgründe des § 112 Abs. 2 oder Abs. 3 AO vorliegen würde. Von Bedeutung ist insbesondere § 112 Abs. 2 AO. Danach darf die ersuchte Behörde Hilfe nicht leisten, wenn sie hierzu aus rechtlichen Gründen nicht in der Lage ist. Eine Reihe von Gesetzen untersagt den mit dem Gesetzesvollzug befassten Behörden die Auskunft auch gegenüber den Finanzbehörden und ordnet ausdrücklich an, dass § 93 AO nicht gilt. Beispielhaft sei hier § 16 Abs. 1 Satz 3 BStatG genannt. Im Gegensatz dazu ist bei Steuerstrafverfahren eine Auskunftspflicht i.d.R. immer gegeben.

Vorstehende Ausführungen gelten für sogenannte Einzelauskunftsersuchen, also Anfragen der Finanzbehörden, die sich auf einen konkret bezeichneten Steuerpflichtigen beziehen.

Eine andere Beurteilung ist bei so genannten Sammelauskunftsersuchen vorzunehmen, bei denen der Kreis der davon Betroffenen zum Zeitpunkt der Anfrage noch nicht feststeht. Bei derartigen Sammelauskunftsersuchen ist nach ständiger Rechtsprechung der Finanzgerichtsbarkeit Voraussetzung, dass ein hinreichender Anlass besteht. Ein solcher liegt vor, wenn aufgrund konkreter Anhaltspunkte oder aufgrund allgemeiner Erfahrung die Möglichkeit einer Steuerverkürzung in Betracht kommt. Ermittlungen „ins Blaue hinein" sind dagegen nicht zulässig. Soweit die Möglichkeit einer Steuerverkürzung im Raum steht, dürften die Ermittlungen in der Regel durch die bei den Finanzämtern eingerichteten Steuerfahndungsstellen durchgeführt werden; im Rahmen einer Steuerfahndung gilt die Einschränkung des § 93 Abs. 1 Satz 3 AO gem. § 208 Abs. 1 AO aber ausdrücklich nicht.

Ich empfehle den betroffenen staatlichen und kommunalen Behörden, Auskunftsersuchen von Finanzbehörden unter Einbeziehung der dortigen Gegebenheiten anhand dieser Hinweise durch den behördlichen Datenschutzbeauftragten überprüfen zu lassen.

15.3 Veröffentlichung von strafbewehrten Unterlassungserklärungen in den Mitteilungsschriften der Steuerberaterkammern München und Nürnberg

In meinem 18. Tätigkeitsbericht (Nr. 11.2) habe ich ausführlich meine datenschutzrechtliche Bewertung der personenbezogenen Veröffentlichungspraxis bei Verurteilungen und strafbewehrten Unterlassungserklärungen in den Mitteilungsschriften der Steuerberaterkammern dargestellt. Ich habe die damalige Veröffentlichungspraxis als nicht zulässig angesehen und nach Art. 31 Abs. 1 BayDSG formell beanstandet. Die Steuerberaterkammern München und Nürnberg haben mir im Hinblick auf meine Bewertung mitgeteilt, dass sie die Veröffentlichungspraxis einschränken werden.

Durch eine Eingabe wurde ich nun auf das von der Steuerberaterkammer München derzeit verwendete Formular einer Unterlassungserklärung aufmerksam. Unter Nummer 3 des Vordrucks findet sich folgender Text: „Der Steuerberaterkammer wird gestattet, die Abgabe dieser Unterlassungserklärung in den Kammermitteilungen der Steuerberaterkammer ... zu veröffentlichen". Es folgt die Unterschrift des Betroffenen.

Aus dem erwähnten Vordruck ergibt sich, dass die Steuerberaterkammer von den Betroffenen die Einwilligung zur Veröffentlichung der Tatsache der Abgabe einer Unterlassungserklärung in den Kammermitteilungen verlangt.

Gemäß Art. 15 Abs. 1 Nr. 2 BayDSG sind zwar die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, wenn der Betroffene einwilligt. Allerdings sind in Art. 15 Abs. 2 bis Abs. 4 BayDSG weitere Voraussetzungen genannt. Insbesondere ist in diesem Zusammenhang Art. 15 Abs. 2 BayDSG zu nennen. Danach ist der Betroffene bei Einholung der Einwilligung auf den Zweck der Erhebung, Verarbeitung und Nutzung, auf die Empfänger vorgesehener Übermittlungen sowie unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern kann. Weiterhin bestimmt Abs. 4, dass in den Fällen, in denen die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt wird, die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben ist.

Die genannten Voraussetzungen sind bei der als Muster übermittelten Unterlassungserklärung nicht gegeben.

Die Steuerberaterkammer München hat im weiteren Verlauf der Diskussion die Ansicht vertreten, bei der Einholung der Einwilligung eines Betroffenen sei dieser nur auf sein Verlangen auf die Darlegung der Rechtsfolgen der Verweigerung der Einwilligung hinzuweisen.

Diese Ansicht findet weder im Gesetzestext noch in der Kommentarliteratur eine Stütze. Nach dem eindeutigen Wortlaut des Art. 15 Abs. 4 BayDSG gilt weiterhin, dass dem Betroffenen - auch ohne dessen ausdrückliches Verlangen - darzulegen ist, welche Folgen die Verweigerung seiner Einwilligung hat.

Weiterhin bin ich der Meinung, dass, nachdem das eingangs erwähnte Formular neben der Einwilligung noch andere Erklärungen des Betroffenen enthält, die Einwilligungserklärung deutlicher hervorzuheben ist. Dies kann bspw. durch einen größeren Schrifttyp oder durch Fettdruck geschehen.

Ich habe deshalb gegenüber der Steuerberaterkammer München deutlich gemacht, dass ich, sofern das augenblickliche Verfahren nicht datenschutzgerecht umgestaltet wird, eine erneute Beanstandung erwäge.

15.4 Heilwasserentnahme aus staatlichen Quellen mittels Chipkartensystem

Der Freistaat Bayern ist Eigentümer der insgesamt drei Heil- und Mineralquellen auf dem Gebiet der Stadt Bad Brückenau; er betreibt durch die Staatliche Kurverwaltung Bad Brückenau das Staatsbad Bad Brückenau, einen Regiebetrieb gem. Art. 26 der Bayerischen Haushaltsordnung. Auf dem Gelände des Kurparks liegt eine Wasserausgabestelle an der Wandelhalle, die der freien Versorgung der Kurpatienten zur Durchführung von Trinkkuren dient.

Bis ins Jahr 2003 hinein hatte die Staatliche Kurverwaltung die unbeschränkte Entnahme von Heilwasser auch anderen Personen gestattet. Nach verschiedenen Vorfällen - wie bspw. dem Abfüllen größerer Wassermengen durch Ortsfremde verbunden mit tumultartigen Zuständen und Gewaltausübungen gegenüber Kurgästen und Mitarbeitern der Kurverwaltung - wurde die Wasserausgabestelle zunächst ganz geschlossen und erst Mitte 2003 - allerdings unter Begrenzung der Öffnungszeit und der Wasserabgabemenge - wieder geöffnet.

Im November 2003 führte die Staatliche Kurverwaltung an der Heilwasserzapfstelle ein Chipkartensystem ein. Nach Bezahlung einer angemessenen Verwaltungsgebühr können Bürger zeitlich und mengenmäßig limitiert Heilwasser entnehmen. Aus traditioneller Verbundenheit räumte die Staatliche Kurverwaltung den Bürgern der Stadt Brückenau und einiger Umlandgemeinden „ohne Anerkennung einer Rechtspflicht“ und ohne Erhöhung der Verwaltungsgebühr im Februar 2004 die Möglichkeit ein, ein erhöhtes Kontingent an Heilwasser zu entnehmen.

Um in den Genuss dieser Vergünstigung zu kommen, muss der Bürger einen Antrag auf eine „Heilquellenkarte“ (Chipkarte) stellen. Dazu muss er - unter Vorlage des Personalausweises - die Daten Vorname, Name, Straße, Postleitzahl, Ort, Geburtsdatum und Personalausweisnummer angeben. Zudem wird mit einer Digitalkamera ein Foto des Antragstellers aufgenommen und mit dem Datensatz abgespeichert. Auf der Chipkarte sichtbar aufgedruckt sind Vorname, Name und Foto des Berechtigten. Zur Wasserentnahme muss der Bürger die Chipkarte in ein an der Wasserentnahmestelle befindliches Terminal stecken. Auf dem Chip der Karte werden die Daten Kundennummer, Gültigkeit, Tageskontingent und Jahreskontingent abgelegt; am Terminal werden die Daten Kundennummer, Datum und Uhrzeit sowie Abgabemenge erfasst. Bei einer Rückgabe der Chipkarte wird diese vor dem Kunden vernichtet; sodann werden die abgespeicherten Daten gelöscht. Die durch Vorlage der „Heilquellenkarte“ und des Personalausweises nachzuweisende Berechtigung der Entnehmenden wird stichprobenartig von den Kurwarten der Staatlichen Kurverwaltung an der Wasserentnahmestelle kontrolliert.

Ein verbrieftes Recht der „Einheimischen“ zur kostenfreien Entnahme von Heilwasser besteht nicht. Der „Wasserstreit“ zwischen den „Einheimischen“ und dem Freistaat Bayern schwelt bereits seit über einem Jahrhundert, ohne dass es zu einer endgültigen gerichtlichen Klärung gekommen wäre.

Der geschilderte Sachverhalt war Gegenstand einer Eingabe an mich. Diese Eingabe habe ich datenschutzrechtlich wie folgt bewertet:

Nach Art. 16 Abs. 1 BayDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist. Gemäß Art. 17 Abs. 1 BayDSG ist das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind.

„Erhebende“ und „speichernde Stelle“ ist hier die Staatliche Kurverwaltung Bad Brückenau. „Aufgabe“ der Staatlichen Kurverwaltung Bad Brückenau ist im

vorliegenden Fall die den Kurbetrieb möglichst gering beeinträchtigende Heilwasserabgabe an Nicht-Kurpatienten.

„Erforderlich“ ist eine Datenerhebung dann, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint. Die Datenkenntnis muss also zum einen zur Aufgabenerfüllung (Erhebungszweck) objektiv beitragen, d.h. die Aufgabenerfüllung ermöglichen, unterstützen oder fördern; maßgeblich ist also die Sachdienlichkeit. Auch eine rein zeitliche Beschleunigung genügt. Zum anderen müssen sowohl die zu erfüllende Aufgabe wie auch deren konkrete Unterstützung, Förderung oder Beschleunigung in Folge der Datenkenntnis jeweils mit den schutzwürdigen Interessen des Betroffenen an der Nichtverwendung seiner Daten hierfür in einem angemessenen Verhältnis stehend erscheinen. Entsprechendes gilt für die Datenspeicherung und -nutzung.

Unter Berücksichtigung dieser Anforderungen begegnet das von der Staatlichen Kurverwaltung Bad Brückenau gewählte Verfahren materiell keinen datenschutzrechtlichen Bedenken:

Das Erheben und Speichern der personenbezogenen Daten Vorname, Name, Straße, Postleitzahl, Ort, Geburtsdatum und Personalausweisnummer im Antrag ist sachdienlich, um die Identität des Antragstellers als Einwohner/Nicht-Einwohner - dies ist wichtig für die Höhe der Abgabemenge - festzustellen und anhand des vorgelegten Personalausweises auch zu überprüfen.

Das Anfertigen eines Fotos erleichtert die von den Kurwarten an der Wasserentnahmestelle vorzunehmende stichprobenartige Kontrolle der Berechtigung des Zapfenden. Da die Heilwasserabgabe ohne Rechtspflicht erfolgt und es in der Vergangenheit zudem zu erheblichen Missbräuchen gekommen ist, ist der Wunsch der Staatlichen Kurverwaltung nach einer Kontrollmöglichkeit nachvollziehbar. Die Staatliche Kurverwaltung kann durch das Foto insbesondere sicherstellen, dass nicht der jeweilige physische Inhaber der „Heilquellenkarte“, sondern nur der Berechtigte das Heilwasser entnimmt, dass also die „Heilquellenkarte“ nicht einfach weitergegeben wird und eine Kontrolle bei „Vergessen“ des Personalausweises erschwert wird. Letztlich entspricht die „Heilquellenkarte“ einer - üblicherweise zur Erleichterung der Kontrolle mit einem Lichtbild versehenen - persönlichen Zeitkarte von öffentlichen Verkehrsmitteln.

Die auf der Chipkarte abgelegten Daten Kundennummer, Gültigkeit, Tageskontingent und Jahreskontingent und die am Terminal erfassten Daten Kundennummer, Datum und Uhrzeit sowie Abgabemenge dienen dazu, die Einhaltung des von der Staatlichen Kurverwaltung eingeräumten täglichen und jährlichen Abnahmekontingents zu überwachen und die Karte bei Ausschöpfung des Tageskontingents zu sperren. Für diese Zwecke sind die erfassten Daten erforderlich. Positiv ist dabei zu werten, dass am Terminal nur die Kundennummer, nicht aber die Daten Vorname, Name, Geburtsdatum und Anschrift des Zapfenden gespeichert werden.

Schließlich erscheinen auch die zu erfüllende Aufgabe - die den Kurbetrieb möglichst gering beeinträchtigende Heilwasserabgabe an Nicht-Kurpatienten - wie auch deren soeben aufgezeigte konkrete Unterstützung, Förderung oder Beschleunigung in Folge der Datenkenntnis jeweils mit den schutzwürdigen Interessen des Betroffenen an der Nichtverwendung seiner Daten hierfür in einem angemessenen Verhältnis stehend.

Die vom Nicht-Kurpatienten erhobenen Daten beschränken sich auf das zur Durchführung des Chipkartensystems erforderliche Mindestmaß. Zu berücksichtigen ist dabei, dass die „Heilquellenkarte“ selbst neben dem Foto sichtbar nur den Vornamen und den Namen des Berechtigten enthält, was aus Datenschutzsicht für den Fall des Verlustes der Karte zu begrüßen ist. Die Chipkarte wird zudem bei einer Rückgabe vor dem Kunden vernichtet; die gespeicherten Daten werden unverzüglich gelöscht. Hinzuweisen ist auch darauf, dass die erhobenen Daten nur für Zwecke der Kontrolle der Wasserentnahme und nicht anderweitig genutzt werden. In das Recht auf informationelle Selbstbestimmung des Chipkarteninhabers wird damit insgesamt nur so gering wie möglich eingegriffen.

In formeller Hinsicht habe ich der Staatlichen Kurverwaltung allerdings empfohlen, die gemäß Art. 16 Abs. 3 BayDSG erforderlichen Hinweise - v.a. im Hinblick auf neu hinzuziehende Bürger - in den Antrag auf Ausstellung der „Heilquellenkarte“ aufzunehmen.

Aus datenschutzrechtlicher Sicht bestehen aus den genannten Gründen deshalb keine Bedenken gegen das von der Staatlichen Kurverwaltung gewählte Verfahren.

16 Personalwesen

16.1 Personalaktendaten

16.1.1 Vorlage von Personalakten an Verwaltungsgerichte

Mit der Frage, inwieweit die beamtenrechtlichen Bestimmungen des Personalaktenrechts (Art. 100 ff. BayBG) im Rahmen eines gerichtlichen Aktenvorlageverlangens gem. § 99 VwGO zu beachten sind, hat sich ein Staatsministerium an mich gewandt. Im Zuge einer Klage vor dem Verwaltungsgericht wolle der Kläger u.a. auch die Rechtmäßigkeit der Ernennung eines Beamten überprüfen lassen. Das Verwaltungsgericht habe deshalb das Staatsministerium als personalaktenführende Stelle mit Formularschreiben zur Vorlage „der vollständigen Originalakten“ aufgefordert. Der Kläger habe aber nicht geltend gemacht, durch die Ernennung des Beamten in eigenen Rechten verletzt worden zu sein.

Diesen Sachverhalt habe ich datenschutzrechtlich wie folgt bewertet:

Die Vorlage von Personalakten an andere Behörden ist zwar grundsätzlich in Art. 100 e Abs. 1 BayBG geregelt; diese Vorschrift ist aber nicht abschließend. Im Falle der Vorlage von Personalakten an Verwaltungsgerichte geht § 99 VwGO dem Art. 100 e Abs. 1 BayBG als Spezialvorschrift vor.

Nach § 99 Abs. 1 Satz 1 VwGO sind Behörden im verwaltungsgerichtlichen Verfahren zur Vorlage von Akten verpflichtet. Wenn das Bekanntwerden des Inhalts dieser Akten allerdings dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheimgehalten werden müssen, kann die zuständige oberste Aufsichtsbehörde die Vorlage der Akten gem. § 99 Abs. 1 Satz 2 VwGO verweigern.

Die Personalakte wurde schon früher zu den ihrem Wesen nach geheimhaltungsbedürftigen Vorgängen gezählt (vgl. nur BVerwGE 19, 179); nunmehr ist die Vertraulichkeit in Art. 100 a Abs. 1 Satz 1 BayBG gesetzlich festgeschrieben. Gemäß § 99 Abs. 1 Satz 2 VwGO kann deshalb die Aktenvorlage nach pflichtgemäßem Ermessen verweigert werden. Das Gericht kann im Verfahren nach § 99 Abs. 2 VwGO die Weigerungserklärung der Behörde daraufhin nachprüfen, ob überwiegende Interessen der Wahrheitsfindung in dem anhängigen Hauptverfahren die Vorlage der Akte trotz ihres vertraulichen Charakters gebieten (BVerwGE 19, 179).

Bei der Ermessensentscheidung ist zwischen der im dienstlichen und im schutzwürdigen persönlichen Interesse des Beamten liegenden Vertraulichkeit der Personalakte seinerseits und dem öffentlichen Interesse an der Wahrheitsfindung in dem vom Untersuchungsgrundsatz beherrschten Verwaltungsprozess andererseits abzuwägen.

Für die Abwägung gelten folgende Grundsätze (vgl. Weiß/Niedermaier/ Summer/Zängl, BayBG, Kommentar, München/Berlin, Stand: 2003, Art. 100 e BayBG Erl. 9):

1. Bei einem Rechtsstreit zwischen dem Beamten und seinem Dienstherrn in einer dienstlichen Angelegenheit ohne Verfahrensbeteiligung eines Dritten stehen grundsätzlich der Aktenvorlage keine Geheimhaltungsgründe entgegen, da den Verfahrensbeteiligten der Akteninhalt ohnehin zugänglich ist. Sofern der Personalakt für die gerichtliche Entscheidung benötigt wird, wäre deshalb eine Verweigerung der Aktenvorlage regelmäßig ermessensfehlerhaft.

2. Anders ist es bereits bei einer Verwaltungsstreitsache zwischen dem Beamten und seinem Dienstherrn, die nicht im Dienstverhältnis ihrer Grundlage findet. Hier dürfte bei einer Abwägung zwischen dem Geheimhaltungsbedürfnis und den Gründen, die für eine Aktenvorlage sprechen, das Geheimhaltungsinteresse des Beamten regelmäßig überwiegen. Dies gilt insbesondere, aber nicht nur dann, wenn sich der Beamte gegen die Beiziehung der Personalakte ausspricht.

3. Generell kommt im Rahmen der Abwägung dem Geheimnisschutz ein erhöhtes Gewicht zu, wenn ein Dritter - und sei es auch nur ein Beigeladener - am Verfahren beteiligt ist.

4. Im Verfahren über eine beamtenrechtliche Konkurrentenklage wird von der Rechtsprechung dagegen die Vorlage des Personalaktes - in gewissen Grenzen - für zulässig gehalten.

5. Anders ist es allerdings, wenn in einem verwaltungsgerichtlichen Verfahren die Vorlage des Personalakts eines unbeteiligten oder beigeladenen Beamten begehrt wird. Hier überwiegt regelmäßig das Geheimhaltungsinteresse. Der Einblick in den Personalakt eines unbeteiligten Beamten würde das verfassungsrechtlich in Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG bzw. Art. 100 BV i.V.m. Art. 101 BV geschützte Recht auf informationelle Selbstbestimmung des Beamten verletzen (vgl. BVerwGE 19, 179).

Im vorliegenden Fall handelte es sich nicht um eine beamtenrechtliche Konkurrentenklage. Auch hat der Kläger nicht geltend gemacht, durch die Ernennung des Beamten in eigenen Rechten verletzt worden zu sein; überdies waren solche Rechte - vor allem im Hinblick auf die viele Jahre zurückliegende Ernennung - nicht erkennbar.

In Anbetracht dieser Sachlage dürfte im Rahmen der nach § 99 Abs. 1 Satz 2 VwGO vom Staatsministerium eigenständig vorzunehmenden Abwägung das in Art. 100 a Abs. 1 Satz 1 BayBG gesetzlich festgehaltene Interesse des Beamten an der Geheimhaltung seiner Personalakten das Interesse des Klägers an der Vorlage des Personalakts eines Dritten überwiegen. Die vorliegende Fallkonstellation entspricht weitgehend der oben unter 5. angeführten Fallgruppe. Im Rahmen der Abwägung ist auch meiner Auffassung nach zu Lasten des seinerzeitigen Klägers zu berücksichtigen, dass dieser im Falle der Vorlage des Personalaktes gem. § 100 Abs. 2 Satz 1 VwGO die Möglichkeit erhalten hätte, sich ohne jede rechtliche Beschränkung Ausfertigungen, Auszüge und Abschriften erteilen zu lassen.

Im Ergebnis berechtigen also meiner Meinung nach die strikten beamtenrechtlichen Bestimmungen des Personalaktendatenschutzes (Art. 100 ff. BayBG) die oberste Aufsichtsbehörde in der Regel dazu, die von einem Verwaltungsgericht angeordnete Vorlage von Personalakten in einem Verfahren, in dem der Betroffene weder Partei noch Konkurrent einer Partei ist, nach § 99 Abs. 1 Satz 2 VwGO aus Gründen der Geheimhaltung zu verweigern.

16.1.2 Bekanntgabe von Leistungsstufen, -prämien und -zulagen

Auf der Basis der damals geltenden einschlägigen Verwaltungsvorschriften habe ich in Nr. 12.1.2 meines 19. Tätigkeitsberichts die Auffassung vertreten, dass der Personalrat im Hinblick auf seine gesetzliche Aufgabenstellung einen Anspruch gegenüber dem Dienststellenleiter hat, dass dieser ihm die Namen der Beschäftigten mitteilt, die eine Leistungsstufe erhalten haben oder in einer Stufe verbleiben. Gleiches gilt für die Vergabe von Leistungsprämien und Leistungszulagen. Dies darf zum Schutz der Empfänger allerdings nur in der Weise geschehen, dass lediglich Einblick in entsprechende Unterlagen innerhalb der Dienststelle gewährt wird. Eine Aushändigung dieser Unterlagen hat zu unterbleiben.

In Teil 16 (Leistungsbesoldung) der seit 01.01.2002 geltenden Bayerischen Verwaltungsvorschriften zum Besoldungsrecht und Nebengebieten (BayVwVBes) ist nunmehr festgelegt, dass die **Personalvertretungen bereits vor der konkreten Vergabeentscheidung zu informieren** sind. Zur Wahrnehmung seiner Aufgabe, zusammen mit der Dienststelle dafür zu sorgen, dass alle in der Dienststelle tätigen Personen nach Recht und Billigkeit behandelt werden, insbesondere, dass jede unterschiedliche Behandlung wegen der Abstammung, Religion, Nationalität, Herkunft, politischen oder gewerkschaftlichen Tätigkeit oder Einstellung oder wegen des Geschlechts unterbleibt, ist der Personalrat vorab zu informieren, welche Beschäftigten eine Leistungsprämie oder Leistungszulage erhalten sollen (Art. 69 Abs. 2, Art. 68 Abs. 1 BayPVG). Die Dienststelle ist aber nicht verpflichtet, dem Personalrat die Erwägungen darzulegen, die den jeweils getroffenen Entscheidungen zugrunde liegen. Der Grundsatz der vertrauensvollen Zusammenarbeit gebietet es, dass der Personalrat Gelegenheit hat, vor der Entscheidung seine Überlegungen vorzutragen. Die Mitglieder der Personalvertretungen haben nach Maßgabe des Art. 10 BayPVG über die ihnen bekannt gewordenen Tatsachen Stillschweigen zu bewahren. Diese Hinweise gelten bei der Vergabe von Leistungsstufen und bei Verbleibensentscheidungen entsprechend.

Meiner Ansicht nach ist diese Verfahrensweise aus Gründen der Gleichbehandlung auch auf den Tarifbereich zu übertragen.

Ergänzend mache ich darauf aufmerksam, dass der Grundsatz der vertrauensvollen Zusammenarbeit es auch gebietet, die Personalvertretungen zu beteiligen, wenn in einer Dienststelle **allgemeine Vergabegrundsätze** aufgestellt werden. Dazu gehört insbesondere die frühzeitige und umfassende Information sowie die Einräumung der Gelegenheit zu Stellungnahme und Erörterung.

Darüber hinaus habe ich in dem eingangs erwähnten Beitrag zum 19. Tätigkeitsbericht ausgeführt, dass eine **Bekanntgabe der Namen der Empfänger** von Leistungsstufen, -prämien oder -zulagen innerhalb einer Behörde, beispielsweise im internen Mitteilungsblatt, **ohne Einwilligung** der Betroffenen **unzulässig** ist. Da diese leistungsbezogenen Zahlungen Bestandteil der Bezüge sind, handelt es sich um Personalaktendaten, die nur für Zwecke der Personalverwaltung oder der Personalwirtschaft unter Berücksichtigung des Erforderlichkeitsgrundsatzes verwendet werden dürfen.

Zwischenzeitlich ist auch in Teil 16 der BayVwVBes festgehalten, dass jede Entscheidung über die Vergabe leistungsbezogener Besoldungsbestandteile Teil des Personalakts und deshalb vertraulich zu behandeln ist (Art. 100 a Abs. 1 Satz 1 BayBG). Eine öffentliche Bekanntgabe ist gemäß Art. 100 e Abs. 2 BayBG ohne entsprechende (vorherige) Einwilligung des betroffenen Beamten unzulässig.

16.1.3 Akteneinsichtsrecht bei Konkurrentenstreitigkeiten

In Anbetracht der aktuellen Entwicklungen im Bereich der beamtenrechtlichen Konkurrentenstreitigkeiten ist es mir ein Anliegen, diese Thematik auch unter dem Blickwinkel des Datenschutzrechts aufzugreifen.

Unter Bezugnahme auf eine frühere Abstimmung mit dem Staatsministerium der Finanzen vertrete ich zum **Akteneinsichtsrecht bei Konkurrentenstreitigkeiten** um die Besetzung eines Beförderungsdienstpostens **vor Einleitung eines Widerspruchs- bzw. gerichtlichen Verfahrens** folgende Auffassung:

1. Das **Protokoll einer Vorstellungskommission oder eines anderen Auswahlgremiums** zählt aufgrund seiner Zweckbestimmung zu den Unterlagen, die dem Stellenbesetzungsverfahren und damit den Sachakten zuzuordnen sind. Die Einsichtnahme in das betreffende Protokoll, das Daten des favorisierten Bewerbers und der Mitbewerber enthält, richtet sich folglich nach Art. 29 BayVwVfG. Da bei der Auswahl eines Bewerbers für einen Beförderungsdienstposten nach Eignung, Befähigung und fachlicher Leistung zu entscheiden ist und dieses Protokoll die Bewertung der Bewerber einschließlich eines abwägenden Vergleichs enthält, ist ein **rechtliches Interesse des Konkurrenten auf Einsicht grundsätzlich zu bejahen**. Nach der Rechtsprechung des Bundesverwaltungsgerichts dürfte dem Konkurrenten hinsichtlich der Kenntnis der vergleichenden Wertungen ein höheres Interesse als dem Geheimhaltungsinteresse des favorisierten Bewerbers einzuräumen sein. Dies gilt jedenfalls, soweit sich die Einsicht auf ihn und den favorisierten Mitbewerber bezieht.

2. Sollte der Konkurrent dagegen **Auskunft aus Personalakten, insbesondere aus Beurteilungen** des erfolgreichen Konkurrenten begehren, ist von Folgendem auszugehen:

   Beurteilungen sind geheimhaltungsbedürftige Personalaktendaten im Sinne des Art. 100 a Abs. 1 Satz 2 BayBG. Die Auskunftserteilung an Dritte, zu denen auch der Konkurrent gehört, richtet sich nach Art. 100 e Abs. 2 BayBG. Danach dürfen Auskünfte an Dritte **nur mit Einwilligung** des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. Inhalt und Empfänger der Auskunft sind dem Beamten schriftlich mitzuteilen. **Willigt der Beamte** also **nicht ein**, können **Auskünfte nur unter engen Voraussetzungen** erteilt werden:

   - Zum Schutz der Interessen Dritter ist eine Auskunft nur nach **sorgfältiger Rechtsgüterabwägung** zulässig. Das Informationsinteresse des Dritten muss berechtigt und nach der Rechtsgüterabwägung höher einzustufen sein als das Geheimhaltungsinteresse des Beamten. Außerdem muss die begehrte Auskunft zum Schutz des Drittinteresses zwingend erforderlich sein; für den Dritten dürfen keine realisierbaren Wege bestehen, um seine Interessen auch ohne die begehrte Auskunft ausreichend wahren zu können. Eine Anhörung des Beamten vor der Erteilung der Auskunft ist nicht (zwingend) vorgeschrieben, entspricht aber der beamtenrechtlichen Fürsorgepflicht, solange dadurch der Zweck der erbetenen Auskunft nicht gefährdet wird. Gleichgültig, ob der Beamte vorher gehört wurde oder nicht, sind ihm jedenfalls Inhalt und Empfänger der Auskunft schriftlich mitzuteilen.

   - Ein **berechtigtes Interesse** des Dritten an der Auskunftserteilung lässt sich zumindest dann bejahen, wenn die getroffene Personalentscheidung angreifbar erscheint. Wenn aber bereits das Protokoll des Auswahlgremiums einen so deutlichen Unterschied zum erfolgreichen Bewerber erkennen lässt, dass ein Vorgehen gegen die Entscheidung keinerlei Aussicht auf Erfolg hat, fehlt dem Konkurrenten dieses berechtigte Interesse.

   - Das berechtigte Interesse muss zudem **höherrangiger** als das Interesse des erfolgreichen Beamten an der Geheimhaltung seiner Personalaktendaten sein. Dieses höherrangigere Interesse ist jedoch grundsätzlich zu verneinen, soweit es dem Konkurrenten vorwiegend um die Beurteilung des Prozess(kosten)risikos geht. Erfolg kann sein Rechtsbehelf nur haben, wenn die Auswahlentscheidung rechtswidrig ist; das ist aber erfahrungsgemäß die Ausnahme. Demgegenüber steht eine immer auch zu berücksichtigende Missbrauchs- und Ausforschungsgefahr, vor

der der erfolgreiche Beamte zu schützen ist. In diesem Zusammenhang darf ich darauf hinweisen, dass Ausforschungsrechte zur besseren Beurteilung des Prozessrisikos unter Einschränkung fremder Grundrechte unserer Rechtsordnung fremd sind. Auch die Berücksichtigung prozessökonomischer Gründe, soweit sie nicht das Kostenrisiko des Konkurrenten, sondern die Belastung der Verwaltungsgerichte betreffen, lässt nach meiner Auffassung der allein auf das Interesse des Auskunft Begehrenden abstellende Wortlaut des Gesetzes („der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert“) nicht zu.

Ob ein berechtigtes, höherrangiges Interesse des Konkurrenten an der Auskunftserteilung gegeben ist, ist also sorgfältig jeweils im Einzelfall zu prüfen.

Diese Auslegung des Art. 100 e Abs. 2 BayBG kann nicht mit der Begründung als „formalistisch“ gekennzeichnet werden, dass der Konkurrent nur Widerspruch gegen die aus seiner Sicht fehlerhafte Auswahlentscheidung einzulegen bräuchte. Auch im Widerspruchsverfahren gibt es kein uneingeschränktes Auskunftsrecht. Vielmehr besteht die Möglichkeit, in den Fällen eines erkennbar nur zum Zweck der Auskunftserteilung „pro forma“ eingelegten oder eines offensichtlich unbegründeten Widerspruchs die Auskunft abzulehnen.

Ergänzend weise ich darauf hin, dass bereits eine große bayerische Kommune mit dieser Problematik befasst war. Diese Kommune gewährt „eine Einsicht in die dienstliche Beurteilung des erfolgreichen Mitbewerbers/der erfolgreichen Mitbewerberin“ erst nach „Widerspruchseinlegung gegen die Stellenbesetzungsentscheidung“. Gegen diese Verfahrensweise habe ich im Hinblick auf meine obige Darstellung keine Einwände erhoben.

Die vorstehenden Grundsätze halte ich auch bei der Besetzung eines nicht mit einer Beförderung verbundenen Dienstpostens für anwendbar.

Zur Vorlage des Personalakts an ein Verwaltungsgericht mache ich auf meine Ausführungen unter Nr. 16.1.1 dieses Tätigkeitsberichts sowie unter Nr. 11.5 meines 15. Tätigkeitsberichts aufmerksam.

16.1.4 Berichtigung und Mitteilung gespeicherter Personalaktendaten

Im Rahmen einer umfangreichen Eingabe hat sich eine Lehrerin bei mir u.a. darüber beschwert, dass die für sie als personalaktenführende Behörde zuständige Regierung in der Personalaktendatei DIAPERS den gesetzlichen Feiertag „Christi Himmelfahrt“ als krankheitsbedingten Fehltag eingetragen habe. Trotz ihrer wiederholt schriftlich vorgetragenen Bitte um Löschung dieses Eintrags und Übersendung eines korrigierten DIAPERS-Datenblattes habe die Regierung über mehrere Jahre hinweg weder den angeblichen Fehltag gelöscht noch ihr ein korrigiertes Datenblatt übersandt. Vielmehr habe ihr die Regierung mitgeteilt, bis zum endgültigen Abschluss mehrerer zwischen ihr und dem Freistaat inzwischen gerichtlich ausgetragener Rechtsstreitigkeiten von der Beantwortung ihrer Schreiben abzusehen. Auf den von ihr gegen diese Mitteilung der Regierung eingelegten „Widerspruch“ habe ihr die Regierung lediglich geantwortet, dass „wir auf Grund der Arbeitsüberlastung und des gegenwärtigen Personalmangels uns außerstande sehen, in absehbarer Zeit den Widerspruchsbescheid zu erstellen.“ Die betroffene Regierung hat mir diesen Sachverhalt bestätigt und ein korrigiertes und aktualisiertes DIAPERS-Datenblatt übersandt.

Nach § 4 Abs. 3 Satz 2 der „Dienstvereinbarung über die Einführung und Anwendung des Personal- und Stellenverwaltungssystems DIAPERS.GX bei den Behörden der allgemeinen inneren Verwaltung“ hat jeder Beschäftigte das Recht, jederzeit einen Ausdruck über den vollständigen, ihn als Person betreffenden Datenbestand sowie über die Stellen, an die Daten regelmäßig übermittelt werden, zu verlangen.

Durch die mehrmalige Verweigerung der von der Lehrerin beantragten Übersendung des DIAPERS-Datenblattes hat die Regierung gegen diese rechtliche Verpflichtung verstoßen. Es wäre der Regierung unschwer möglich gewesen, jedenfalls den offensichtlich unzutreffenderweise als krankheitsbedingten Fehltag in DIAPERS eingetragenen Feiertag „Christi Himmelfahrt“ zu löschen und der betroffenen Lehrerin ein insoweit korrigiertes DIAPERS-Datenblatt zukommen zu lassen.

Aus diesem Grund habe ich den wiederholten Verstoß gegen § 4 Abs. 3 Satz 2 der DIAPERS-Dienstvereinbarung gem. Art. 31 Abs. 1 BayDSG förmlich beanstandet. Der Eingabeführerin habe ich den korrigierten und aktualisierten DIAPERS-Ausdruck zugesandt. Ich gehe davon aus, dass die Regierung der Lehrerin nach endgültigem Abschluss der Rechtsstreitigkeiten ein (ggf. neuerlich) aktualisiertes DIAPERS-Datenblatt übermittelt.

16.2 Personaldaten im Gemeinderat

Im Berichtszeitraum häuften sich Anfragen von Kommunen zur Nutzung von Personaldaten durch den Gemeinderat. Dabei ging es v.a. um die Unterrichtung über Schwangerschaften, die Einsicht in Geschäftsverteilungsplan und Stellenbeschreibung oder um die Mitteilung der Höhe von Überstunden und Resturlaub der Gemeindebediensteten. Aber auch Veröffentlichungen aus dem Gemeinderat, wie die Bekanntgabe von Sachbearbeiternamen gegenüber der örtlichen Presse, waren ein Thema. In Anbetracht der allgemeinen Bedeutung solcher Fallgestaltungen gebe ich aus datenschutzrechtlicher Sicht folgende Hinweise:

Nutzung von Personaldaten durch den Gemeinderat

Der Gemeinderat ist (einschließlich seiner Ausschüsse) Teil der öffentlichen Stelle „Gemeindeverwaltung". Die Weitergabe personenbezogener Daten von der (sonstigen) Gemeindeverwaltung an den Gemeinderat stellt daher eine Datennutzung gemäß Art. 4 Abs. 7 BayDSG dar.

Die Zulässigkeit der Weitergabe personenbezogener Daten an den Gemeinderat ist grundsätzlich nach Art. 17 BayDSG zu beurteilen, soweit keine spezielleren Rechtsvorschriften vorgehen.

Eine solche vorrangige Rechtsvorschrift stellt Art. 100 a Abs. 1 Satz 3 BayBG dar, der meiner Auffassung nach analog auch auf die nicht verbeamteten Beschäftigten des öffentlichen Dienstes anzuwenden ist, da er allgemein gültige Schutzprinzipien für Arbeitnehmer enthält. Nach dieser Bestimmung dürfen Personalaktendaten (vgl. Art. 100 a Abs. 1 Satz 2 BayBG) - beispielsweise über eine Schwangerschaft, aber auch über Überstunden und Urlaub - nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein. Die Begriffe „Personalverwaltung" und „Personalwirtschaft" sind hier weit gefasst. Personalaktendaten dürfen danach nicht nur für auf den einzelnen Beamten bezogene Zwecke, sondern auch für allgemeine Zwecke der Personalverwaltung und Personalwirtschaft herangezogen werden, soweit dafür Personalaktendaten einzelner oder sämtlicher Beamten benötigt werden. Im Übrigen kommt man zum gleichen Ergebnis, wenn man bei Angestellten und Arbeitern ohne analoge Anwendung des Personalaktenrechts für Beamte Art. 17 Abs. 1 BayDSG anwendet, der sowohl das Erforderlichkeitsprinzip als auch das Zweckbindungsprinzip enthält.

Um die Frage der datenschutzrechtlichen Zulässigkeit beantworten zu können, ist es also notwendig, die Gründe für die Information des Gemeinderats zu ermitteln. Nur dann kann die Erforderlichkeit der Datennutzung geprüft werden. Zu berücksichtigen ist dabei auch der Adressat der Datennutzung; u.U. ist eine Datennutzung durch den zuständigen Ausschuss, wie hier den Personalausschuss, ausreichend.

In Anbetracht der genannten Zwecke sind meiner Ansicht nach Fälle denkbar, in denen dem Gemeinderat (Personalausschuss) - unter Wahrung des Grundsatzes der Erforderlichkeit - die **Schwangerschaft** einer Mitarbeiterin ohne deren vorherige Zustimmung mitgeteilt werden oder Einsicht in den **Geschäftsverteilungsplan und** in die **Stellenbeschreibung** gewährt werden darf.

Was dagegen die Forderung nach Mitteilung der Höhe von **Überstunden und Resturlaub** sämtlicher Gemeindebediensteten an den Gemeinderat betrifft, ist insbesondere auf Art. 37 Abs. 4 und Art. 43 Abs. 3 GO hinzuweisen. Danach führt der erste Bürgermeister die Dienstaufsicht über die Beamten, Angestellten und Arbeiter der Gemeinde; er ist zudem Dienstvorgesetzter der Gemeindebeamten. Die Befugnisse des Gemeinderats in Personalangelegenheiten sind hingegen in Art. 43 Abs. 1 GO enumerativ begrenzt und können zudem gem. Art. 43 Abs. 2 GO auf den ersten Bürgermeister übertragen werden. Vor diesem Hintergrund lässt sich aus meiner Sicht die namentliche Mitteilung der Höhe von Überstunden und Resturlaub an den Gemeinderat (Personalausschuss) weder Zwecken der Personalverwaltung oder der Personalwirtschaft gemäß Art. 100 a Abs. 1 Satz 3 BayBG zuordnen, noch kann ich deren Erforderlichkeit erkennen. Ein denkbares Interesse des Gemeinderats an der Zahl der Überstunden und der Resturlaubstage kann anonymisiert erfüllt werden.

Im Übrigen hat der Gemeinderat gegenüber dem ersten Bürgermeister ein Informationsrecht, soweit die Datenweitergabe zum Vollzug seiner Aufgaben erforderlich und damit zulässig ist. Diesem Informationsrecht setzt der Erforderlichkeitsgrundsatz des Art. 17 Abs. 1 Nr. 1 BayDSG Grenzen. Ziel von Überwachungsmaßnahmen nach Art. 30 Abs. 3 GO kann stets nur die Gewährleistung der Gesetzmäßigkeit der Verwaltung sein. Es bedarf also eines sachlich begründeten Anlasses, der eine Kontrolle erforderlich macht.

Veröffentlichungen aus dem Gemeinderat

Gegen die ortsübliche Veröffentlichung der Niederschriften öffentlicher Gemeinderatssitzungen, die lediglich den in Art. 54 Abs. 1 GO vorgesehenen Mindestinhalt enthalten, bestehen keine datenschutzrechtlichen Einwendungen. Da die Veröffentlichung personenbezogener Daten durch die Gemeinde datenschutzrechtlich eine Datenübermittlung an nicht-

öffentliche Stellen darstellt, ist eine weiter gehende Information der Öffentlichkeit über den Ablauf einer Sitzung grundsätzlich nach Art. 19 Abs. 1 BayDSG zu beurteilen. Allerdings geht eine Reihe spezieller Geheimhaltungsvorschriften - wie z.B. die Art. 100 ff. BayBG über das Personalaktengeheimnis - dieser allgemeinen Vorschrift vor (vgl. Art. 2 Abs. 7 BayDSG) und stellt erheblich strengere Anforderungen an die Zulässigkeit von Übermittlungen an Dritte.

Gemäß Art. 100 e Abs. 2 Satz 1 BayBG dürfen Auskünfte aus Personalakten an Dritte nur mit Einwilligung des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. Inhalt und Empfänger der Auskunft sind dem Beamten schriftlich mitzuteilen (Art. 100 e Abs. 2 Satz 2 BayBG).

In diesem Zusammenhang ist auch darauf hinzuweisen, dass es zur ordnungsgemäßen Aufgabenerfüllung einer Kommune gehört, die Bürger darüber zu informieren, welche Bediensteten die richtigen Ansprechpartner für ihre Anliegen sind. Dazu ist es zulässig, Bedienstete, die Funktionen mit „Außenwirkung“ in der Verwaltung wahrnehmen, auch namentlich der Öffentlichkeit bekannt zugeben. Dieser Personenkreis muss aufgrund seiner auf die Öffentlichkeit bezogenen Aufgabenstellung daher beispielsweise hinnehmen, dass von ihm Name, Amts-/Dienstbezeichnung, Tätigkeitsbereich und Funktion sowie dienstliche Anschrift und Telefonnummer, z.B. in Form eines „Behördenwegweisers“, veröffentlicht werden (siehe in diesem Zusammenhang auch die Nr. 12.3 meines 18. Tätigkeitsberichts zu Mitarbeiterdaten im Internet und Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, Teil C, Handbuch XII.8.b).

Vor diesem Hintergrund ist bei der **Bekanntgabe von Sachbearbeiternamen gegenüber der örtlichen Presse** allgemein auf Art. 4 Abs. 1 Satz 1 BayPrG hinzuweisen, der unter dem Vorbehalt des Art. 4 Abs. 2 Satz 2 BayPrG steht. Danach darf eine Auskunft nur verweigert werden, soweit aufgrund beamtenrechtlicher oder sonstiger gesetzlicher Vorschriften eine Verschwiegenheitspflicht besteht. Der presserechtliche Auskunftsanspruch steht daher - mit den erwähnten Einschränkungen - unter dem Vorbehalt der Verschwiegenheitspflicht des Dienstherrn nach Art. 100 e Abs. 2 BayBG.

In Bezug auf die (generelle) **Bekanntgabe des Namens des** (jeweils) **zuständigen Sachbearbeiters in einer öffentlichen Sitzung des Gemeinderats** kann ich weder ein Informationsinteresse der Allgemeinheit noch des Gemeinderats erkennen. Meiner Ansicht nach besteht im Rahmen einer öffentlichen Sitzung grundsätzlich keine Erforderlichkeit für die Nennung des Sachbearbeiternamens, insbesondere in dessen Abwesenheit. Über die Tagesordnungspunkte und über die „Arbeit der Beschäftigten“ kann auch ohne deren Namensnennung beraten werden. Gemäß Art. 100 e Abs. 2 BayBG ist eine Namensnennung deshalb regelmäßig nur mit Einwilligung des Betroffenen zulässig.

Zur **Übersendung von Sitzungsunterlagen über Personalangelegenheiten** (z.B. Bewerbungsunterlagen) an die Mitglieder des Gemeinderats (bzw. des Personalausschusses) mache ich auf meine in den Nrn. 7.4 meines 14. Tätigkeitsberichts und 7.3 meines 15. Tätigkeitsberichts vertretene Auffassung, die sich im Übrigen mit der des Staatsministeriums des Innern deckt, aufmerksam. Aus meiner Sicht ist es zur Aufgabenerfüllung der Mitglieder des Gemeinderats (bzw. des Personalausschusses) nicht im Sinne des Art. 17 Abs. 1 Nr. 1 BayDSG erforderlich, Sitzungsunterlagen über Personalangelegenheiten schon zusammen mit der Tagesordnung zu erhalten. Hier besteht die Gefahr, dass in den Sitzungsunterlagen enthaltene vertrauliche Informationen unbefugt an Dritte gelangen oder weitergegeben werden könnten. In Anbetracht der besonderen Sensibilität dieser Daten halte ich daher allein eine Information der Gemeinderats-/Personalausschussmitglieder in der Sitzung selbst für datenschutzrechtlich vertretbar.

16.3 Befugnisse des Dienstherrn bzw. Arbeitgebers

16.3.1 Erhebung personenbezogener Daten über Bewerber

Im Zuge der Veränderungen am Arbeitsmarkt gewinnt die Problematik der Erhebung personenbezogener Daten bei der Auswahl von Bewerbern mehr und mehr an Bedeutung. Aus datenschutzrechtlicher Sicht nehme ich dazu wie folgt Stellung:

Nach Art. 100 Satz 1 BayBG darf der Dienstherr personenbezogene Daten über (Beamten-) Bewerber nur erheben, soweit dies zur Begründung des Dienstverhältnisses erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Fragebogen, mit denen solche personenbezogenen Daten erhoben werden, bedürfen gem. Art. 100 Satz 2 BayBG der Genehmigung durch die oberste Dienstbehörde. Zum Schutz der Bewerber gelten diese Vorschriften bereits im Vorfeld der Einstellung. **Datenschutzrechtlich zulässig ist nur die Erhebung der „erforderlichen“ Daten.** Nötig ist hier stets eine Abwägung zwischen dem Informationsinteresse des Dienstherrn und dem Anspruch des Bewerbers auf Persönlichkeitsschutz.

Dabei ist zu beachten, dass der unbestimmte Rechtsbegriff „erforderlich“ **nicht nur eine materielle, sondern auch eine zeitliche Komponente** umfasst. In materieller Hinsicht müssen die personenbezogenen Daten eine zulässige Entscheidungsgrundlage bilden. In zeitlicher Hinsicht darf der Dienstherr im Rahmen der Bewerbung keine Daten erheben, die für eine Entscheidung über die Einstellung ohne rechtliche Bedeutung sind, selbst wenn sie später für die Durchführung des Dienstverhältnisses benötigt werden. Bei der Bewerbung können somit zum einen die Daten erhoben werden, anhand derer nachgeprüft werden kann, ob die zwingenden (persönlichen) Einstellungsvoraussetzungen erfüllt sind. Benötigt werden zum anderen aber auch diejenigen personenbezogenen Daten, die erforderlich sind, um eine leistungsgerechte Auswahl nach Art. 12 Abs. 2 BayBG zwischen mehreren Bewerbern zu treffen. Schließlich bestehen keine Bedenken gegen die Erhebung von Daten, die für die personalpolitische Ermessenabwägung zwischen mehreren im wesentlich gleich gut geeigneten Bewerbern notwendig sind.

Der Dienstherr darf nach dem **Grundsatz der Verhältnismäßigkeit** nur Daten in einem für die Entscheidungsfindung erforderlichen Ausmaß erheben (also z.B. nicht, um sich ein „lückenloses Bild von der Persönlichkeit des Bewerbers“ zu verschaffen). Dies gilt ebenso hinsichtlich der charakterlichen und der gesundheitlichen Eignung.

Nach den vorstehenden Ausführungen ist es daher **beispielsweise zulässig**, im Rahmen der Bewerbung um eine Einstellung ins Beamtenverhältnis u. a. Unterlagen, Erklärungen und Auskünfte **zur Prüfung der charakterlichen Eignung** - wie z.B. polizeiliche Führungszeugnisse, Auszüge aus dem Bundeszentralregister, Erklärungen über etwaige anhängige Ermittlungsverfahren - zu erheben.

Zur Feststellung der gesundheitlichen Eignung eines Bewerbers ist eine ärztliche Untersuchung erforderlich, welche dem Gesundheitsamt oder einem anderen von der Einstellungsbehörde beauftragten Arzt obliegt. Ergeben sich keine Zweifel an der gesundheitlichen Eignung, darf nur das zusammenfassende Untersuchungsergebnis an den Dienstherrn übermittelt werden. Bestehen allerdings Bedenken gegen die gesundheitliche Eignung, müssen diese auch in dem zusammenfassenden Bericht soweit konkretisiert werden, dass die Einstellungsbehörde darüber befinden kann, ob ergänzende ärztliche Untersuchungen erforderlich sind, ob trotz der getroffenen medizinischen Feststellungen die gesundheitliche Eignung noch bejaht werden kann oder ob die gesundheitliche Eignung nicht mehr Gewähr leistet ist. Es steht grundsätzlich im Ermessen des Dienstherrn, ob bzw. welche gesonderten Untersuchungen hinsichtlich bestimmter Erkrankungen oder Risikofaktoren vorzunehmen sind. Dabei muss aber der Dienstherr zwischen dem eigenen Informationsinteresse und den schutzwürdigen Belangen des Bewerbers abwägen. Eine Grenze für gezielte Untersuchungen ist jedenfalls dort zu ziehen, wo durch eine Untersuchung erheblich in die Intimsphäre eingegriffen würde (z.B. bei einer Genomanalyse zur Ermittlung veranlagungsbedingter Risiken für künftige Erkrankungen).

In diesem Zusammenhang weise ich auch darauf hin, dass eine **Einwilligung** des Betroffenen für sich allein noch keine Datenerhebung rechtfertigt. Auch auf freiwilliger Basis dürfen nur die Daten erhoben werden, die der Dienstherr zulässigerweise verwenden darf.

Meine Ausführungen zu Art. 100 BayBG gelten auch in Bezug auf die **nicht verbeamteten Beschäftigten** des öffentlichen Dienstes; zur analogen Anwendung des Art. 100 BayBG verweise ich auf die Nrn. 13.1.1 und 13.1.2 meines 20. Tätigkeitsberichts. Für die Beurteilung der Datenerhebung kann auch die **Rechtsprechung zum Fragerecht des Arbeitgebers** herangezogen werden. Dem Arbeitgeber steht danach ein Fragerecht zu, wenn er im Zusammenhang mit dem zu begründenden Arbeitsverhältnis ein berechtigtes, billigenswertes und schutzwertes Interesse an der Beantwortung seiner Fragen hat. Das Interesse muss objektiv so stark sein, dass dahinter das Interesse des Bewerbers am Schutz seines Persönlichkeitsrechts und an der Unverletzlichkeit seiner Intimsphäre zurücktritt. Nach Auffassung des Bundesarbeitsgerichts kann der Arbeitgeber daher nach persönlichen Daten des Bewerbers insoweit fragen, als diese in einem Sachzusammenhang mit dem geplanten Arbeitsverhältnis stehen. So darf nach Vorstrafen (auch im öffentlichen Dienst) z.B. nur gefragt werden, soweit die Straftaten für das beabsichtigte Arbeitsverhältnis relevant sind.

Die Bewerbungsunterlagen sind den **Sachakten** zuzuordnen; erst bei einer Einstellung ist ein Personalakt zu führen, in den die Bewerbungsunterlagen aufgenommen werden können (vgl. Art. 100 a Abs. 1 Satz 1 BayBG, § 13 BAT, § 13 a MTArb). In Bezug auf den Verbleib der Bewerbungsunterlagen von nicht zum Zuge gekommenen Bewerbern treffen die o. a. Bestimmungen allerdings keine Regelung. Mangels bereichsspezifischer Vorschriften gelten deshalb für die Verarbeitung und Nutzung personenbezogener Daten von Bewerbern sowie für ihre Auskunftsansprüche die Regelungen des allgemeinen Datenschutzrechts (BayDSG).

16.3.2 Veröffentlichung von Mitarbeiterfotos

Eines der wesentlichen Ziele der Verwaltungsmodernisierung ist die Bürgerorientierung der Verwaltung. Der Bürger soll nicht mehr als bloßer Antragsteller oder Adressat von Verwaltungsakten angesehen werden, sondern wie ein „Kunde“ eines Dienstleistungsunternehmens behandelt werden. In datenschutzrechtlicher Hinsicht war ich im Berichtszeitraum vor allem mit dem damit einhergehenden Wunsch der Dienstherren bzw. Arbeitgeber nach **Veröffentlichung von Fotos der Beschäftigten** befasst. Dazu gebe ich folgende Hinweise:

Nach Art. 15 Abs. 1 BayDSG ist die Veröffentlichung personenbezogener Daten zulässig, wenn die Betroffenen wirksam einwilligen (Nr. 2) oder eine Rechtsnorm sie gestattet (Nr. 1). Als Datenübermittlung an nicht-öffentliche Stellen ist die Veröffentlichung an Art. 19 Abs. 1 Nr. 1 BayDSG zu messen. Entscheidend ist also, ob die Veröffentlichung von Mitarbeiterfotos zur ordnungsgemäßen Aufgabenerfüllung der öffentlichen Stelle erforderlich ist. Sicherlich gehört es zur ordnungsgemäßen Aufgabenerfüllung einer öffentlichen Stelle, die „Kunden“ darüber zu informieren, welche Beschäftigten die richtigen Ansprechpartner für ihre Anliegen sind. Für diese Information ist aber die Veröffentlichung von Mitarbeiterfotos nicht erforderlich. Soweit aber über die zur ordnungsgemäßen Aufgabenerfüllung erforderlichen Daten hinaus personenbezogene Daten veröffentlicht werden sollen, ist die **freiwillige, informierte und schriftliche Einwilligung der Betroffenen** (vgl. Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG) einzuholen.

Zu den Problemkreisen Mitarbeiterdaten im Internet und Personaldaten im Intranet habe ich mich bereits in früheren Tätigkeitsberichten, und zwar in Nr. 12.3 meines 18. und in Nr. 13.1.4 meines 20. Tätigkeitsberichts, grundlegend geäußert. In Anbetracht der weltweiten Verbreitung und der damit verbundenen Missbrauchsgefahr sollte meiner Ansicht nach auf die **Veröffentlichung von Bedienstetenfotos im Internet** selbst bei wirksamer Einwilligung der Betroffenen **verzichtet** werden. Gegen eine Veröffentlichung von Fotos **im Intranet** - natürlich nur mit Einwilligung des Betroffenen - habe ich indes **keine Einwendungen.**

Hinsichtlich der bayerischen Beamten ist ergänzend auf Art. 100 a Abs. 1 Satz 3 sowie Art. 100 e Abs. 2 BayBG hinzuweisen. Das im **Personalakt** enthaltene Foto darf danach ohne Einwilligung des betroffenen Beamten weder innerhalb noch außerhalb der Behörde verwendet werden.

Zur Veröffentlichung von Fotos des **Personals an Schulen** nehme ich auf Nr. 15.1 meines 19. Tätigkeitsberichts Bezug. Dort habe ich festgestellt, dass sowohl die Einstellung von Fotos auf der Homepage einer Schule als auch deren Weitergabe an die (lokale) Presse einer ausdrücklichen **Einwilligung** der betroffenen Beschäftigten bedürfen. Diese sind vorher über die Risiken einer solchen Veröffentlichung zu informieren. In Nr. 4.4 Buchstabe d der Erläuternden Hinweisen für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes (KMBek vom 19.04.2001, KWMBl I S. 112, geändert durch KMBek vom 10.10.2002, KWMBl I S. 354) ist überdies geregelt, dass zur Illustration des **Jahresberichts** (vgl. Art. 85 Abs. 3 BayEUG) auch Lehrerfotos aufgenommen werden können. Voraussetzung dafür ist jedoch auch hier, dass die Betroffenen eingewilligt haben.

Zur Veröffentlichung von **Schülerfotos** habe ich in Nr. 20.1.3 dieses Tätigkeitsberichts Stellung genommen.

Schließlich kommt es auch für die Beurteilung der Zulässigkeit der Veröffentlichung von Fotos von **Mitarbeiterinnen und Mitarbeiter der bayerischen Hochschulen** darauf an, ob die Fotoveröffentlichung zur Erfüllung der in der Zuständigkeit der Hochschule liegenden Aufgaben erforderlich ist. Vor dem Hintergrund meiner Ausführungen zu den „Hinweisen zur Veröffentlichung von Mitarbeiterdaten im Internet für die bayerischen Hochschulen“ unter Nr. 16.2.1 meines 20. Tätigkeitsberichts ist dies regelmäßig zu verneinen. Somit ist auch hier eine **datenschutzrechtlich wirksame Einwilligung der Betroffenen** einzuholen.

16.3.3 Medizinische Gutachten im Beamtenverhältnis

Wie zahlreiche Eingaben und Anfragen belegen, ist in jüngster Zeit die datenschutzrechtliche Problematik medizinischer Gutachten mehr und mehr in den Blickpunkt des Interesses sowohl der bayerischen Beamten wie auch deren Dienstherren gerückt. Mit einer medizinischen Untersuchung können einschneidende Veränderungen im beruflichen und finanziellen Bereich verbunden sein. Aus datenschutzrechtlicher Sicht ist dazu Folgendes festzuhalten:

Dienstfähigkeit

Nach Begründung des Beamtenverhältnisses gehört es zu den Dienstpflichten des Beamten, sich bei Zweifeln an der Dienstfähigkeit auf Anordnung einer amtsärztlichen Untersuchung zu unterziehen. Der allgemeinen Schweigepflicht des Arztes stehen die durch Art. 33 Abs. 5 GG verfassungsrechtlich geschützten Belange des Dienstherrn gegenüber, der seine gesetzlichen Aufgaben nur bei Kenntnis des

Gesundheitszustands des Beamten erfüllen kann. Es ist daher festzustellen, dass der Amtsarzt - soweit er aufgrund einer hoheitlichen Anordnung des Dienstherrn tätig wird - für diesen handelt, nicht für den Beamten.

Ob die ärztlichen Erkenntnisse detailliert an den Dienstherrn weiter gegeben werden müssen oder ob eine zusammenfassende Stellungnahme genügt, hängt von den Umständen des Einzelfalls ab. Dabei ist stets zwischen dem dienstlichen Informationsinteresse und dem persönlichen Geheimhaltungsinteresse unter Beachtung des Grundsatzes der Verhältnismäßigkeit abzuwägen. Die Interessenabwägung gebietet, dass die Dienstbehörde keine weiter gehenden Angaben verlangt als für eine sachgerechte Entscheidung erforderlich. In Zweifelsfällen ist aber der Amtsarzt berechtigt und auf Verlangen verpflichtet, der zuständigen Dienstbehörde nähere medizinische Einzelheiten mitzuteilen.

Nach Art. 11 Abs. 1 des Gesetzes über den öffentlichen Gesundheits- und Veterinärdienst, die Ernährung und den Verbraucherschutz sowie die Lebensmittelüberwachung (Gesundheitsdienst- und Verbraucherschutzgesetz - GDVG) gehört es zu den Aufgaben der Behörden des öffentlichen Gesundheitsdienstes, amtsärztliche Zeugnisse zu erstellen. Eine Rechtsgrundlage dafür stellt beispielsweise § 21 Abs. 2 Satz 2 UrlV dar. Danach haben Beamte zum Nachweis **vorübergehender Dienstunfähigkeit** auf Anordnung des Dienstvorgesetzten ein amtsärztliches Zeugnis beizubringen. Nach Art. 31 Abs. 5 Nr. 1 i.V.m. Art. 30 Abs. 2 Satz 1 Nr. 1 GDVG dürfen die bei der amtsärztlichen Untersuchung gewonnenen Erkenntnisse weiter gegeben werden, wenn dies durch Rechtsvorschrift ausdrücklich zugelassen ist. Somit ist auch eine Datenweitergabe am Maßstab des § 21 Abs. 2 Satz 2 UrlV zu messen.

Eine Regelung über die Mitteilung aus Untersuchungsbefunden findet sich für die Fälle der (amts-) ärztlichen Untersuchung zur **Überprüfung der Dienstfähigkeit im Rahmen einer Ruhestandsversetzung** in Art. 60 a Abs. 1 BayBG. Danach teilt der Arzt im Einzelfall auf Anforderung der Behörde die tragenden Feststellungen und Gründe des Gutachtens und die in Frage kommenden Maßnahmen zur Wiederherstellung der Dienstfähigkeit mit, soweit deren Kenntnis für die Entscheidung der Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit erforderlich ist.

Ergänzend dazu mache ich auf die in den Verwaltungsvorschriften zum Bayerischen Beamtengesetz (VV-BayBG) aufgestellten, mit mir abgestimmten Grundsätze für die Überprüfung der Dienstfähigkeit von Beamten und Richtern aufmerksam. Auch nach Nr. 4 der VV zu Art. 56 ff. BayBG führt die Abwägung zwischen dem dienstlichen Informationsinteresse und dem persönlichen Geheimhaltungsinteresse regelmäßig zu dem Ergebnis, dass der Dienstvorgesetzte nur die für eine sachgerechte Entscheidung erforderlichen Angaben verlangen darf. In Zweifelsfällen ist der begutachtende Arzt aber verpflichtet, der zuständigen Dienstbehörde im Rahmen des für die Entscheidung Erforderlichen auf Verlangen nähere medizinische Einzelheiten mitzuteilen.

Meine Äußerungen unter Nr. 3.5.2 meines 17. Tätigkeitsberichts sind damit überholt.

Personalakt

Nach Art. 100 e Abs. 1 Satz 3 BayBG darf **Ärzten**, die im Auftrag der personalverwaltenden Behörde oder der Pensionsbehörde ein medizinisches Gutachten erstellen, der **Personalakt ohne Einwilligung des Beamten vorgelegt** werden. Die Vorlage ist notwendig, da zur Erstellung medizinischer Gutachten zumeist Personalaktendaten (z.B. Angaben über gesundheitsbedingte Ausfallzeiten) benötigt werden. Die Vertraulichkeit der Personalaktendaten wird durch die ärztliche Schweigepflicht gesichert. Eine Einwilligung des Beamten sieht das Gesetz nicht vor, da weder die ärztliche Begutachtung noch die ggf. darauf gestützte Entscheidung dem Verfügungsrecht des Beamten unterfallen. Aber auch hier gelten die Grundsätze: Auskunft vor Aktenvorlage und Beschränkung auf den jeweils erforderlichen Umfang (vgl. Art. 100 e Abs. 1 Satz 5 und Abs. 4 BayBG).

Dienstunfall

Zum Verfahren in Dienstunfallsachen, das seinerzeit in datenschutzrechtlicher Hinsicht mit mir abgestimmt worden ist, ist Folgendes anzumerken:

Nach Teil 9 (Unfallfürsorge) der Bayerischen Verwaltungsvorschriften zum Versorgungsrecht (BayVV-Versorgung) entscheidet die Pensionsbehörde über die Anerkennung des Unfalles als Dienstunfall und über die Gewährung von Unfallfürsorgeleistungen (§ 45 Abs. 3 BeamtVG). Soweit für die zu treffende Entscheidung ergänzende Sachverhaltsermittlungen erforderlich sind, werden sie von der Pensionsbehörde durchgeführt. In diesem Zusammenhang entscheidet die Pensionsbehörde auch über die Beiziehung ärztlicher Sachverständiger. Zur Feststellung, mit welchem Ergebnis und zu welchem Zeitpunkt das dienstunfallbedingte Heilverfahren als abgeschlossen angesehen werden kann, ist der Verletzte zu hören. Es liegt im Ermessen der Pensionsbehörde, hierzu eine amts-/polizeiärztliche Stellungnahme einzuholen (= sog. Schlussgutachten).

Für die Unfallmeldung sind die zu den BayVV-Versorgung als Anlagen 3 (Dienstunfalluntersu-

chung) und 4 (Beiblatt zur Dienstunfalluntersuchung) beigefügten Vordrucke zu verwenden. In der Anlage 4 findet sich zur Entbindung von der ärztlichen Schweigepflicht/Akteneinsicht eine Erklärung des Verletzten. In Abschnitt IV Nr. 1 dieses Beiblatts entbindet der verletzte Beamte/die verletzte Beamtin die in Abschnitt II und III genannten Ärzte, Krankenanstalten sowie die Krankenversicherung, die Träger der Sozialversicherung und die Behörden des öffentlichen Gesundheitsdienstes gegenüber dem polizei-/amtsärztlichen Dienst, den beizuziehenden ärztlichen Gutachtern und der für die dienstunfallrechtliche Entscheidung zuständigen Bezirksfinanzdirektion von der ärztlichen Schweigepflicht, soweit dies zur sachgerechten Bearbeitung der Dienstunfallangelegenheit erforderlich ist (z.B. zur Einholung von Untersuchungsbefunden). In Abschnitt IV Nr. 2 Spiegelstrich 1 dieses Beiblatts erklärt sich der verletzte Beamte/die verletzte Beamtin durch Unterschrift damit einverstanden, dass die bei der Bezirksfinanzdirektion geführten Dienstunfallunterlagen zur sachgerechten Bearbeitung den beizuziehenden ärztlichen Gutachtern bekannt gegeben werden.

Die Vordrucke sowie Informationen zum Dienstunfall können im Internet unter der Adresse www.bayern.de/Bezirksfinanzdirektionen/formular.htm abgerufen werden. Die dort noch angegebene DUnfBek ist mittlerweile inhaltsgleich durch die BayVV-Versorgung ersetzt worden.

Die Dienstunfalluntersuchung und alle damit in Zusammenhang stehenden Unterlagen werden als Teilakt des Personalakts bei der Pensionsbehörde aufbewahrt (vgl. Art. 100 b Satz 5 BayBG). Eine Einsicht in diese bei der zuständigen Bezirksfinanzdirektion geführten Unterlagen ist nach Maßgabe des Art. 100 d BayBG möglich.

17 Gewerbe und Handwerk

17.1 Novellierung der Gewerbeordnung

1. Regelung von Löschungsfristen für Gewerbeanzeigen

Aufgrund der Novellierung der Gewerbeordnung durch Gesetz vom 24.08.2002 (BGBl I S. 3412 - siehe dazu 20. Tätigkeitsbericht 2002 Nr. 14.1) hat der Bund-Länder-Ausschuss „Gewerberecht“ eine neue Muster-Verwaltungsvorschrift für die Gewerbeanzeige und das Bewachungsrecht beschlossen. Auch die bayerischen Verwaltungsvorschriften, insbesondere die Allgemeine Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung (GewAnzVwV), hatten sich im wesentlichen an dieser Musterfassung orientiert, so dass eine entsprechende Anpassung erforderlich wurde. Im Zuge der Deregulierung hat das Bayerische Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie vom Erlass einer (novellierten) Allgemeinen Verwaltungsvorschrift für den Bereich der Gewerbeanzeigen und des Bewachungsgewerbes abgesehen. Mit Schreiben vom 04.12.2003 wurden den Gewerbebehörden jedoch Hinweise zur Gewerbeanzeige und zum Bewachungsgewerberecht als Hilfestellung an die Hand gegeben. In den Hinweisen wurde zusätzlich zur o.g. Muster-Verwaltungsvorschrift unter Ziffer 6.3.6 eine Regelung über die Aufbewahrungs- und Löschungsfristen für die Gewebeanzeigedaten aufgenommen. Daten aus der Gewerbeanzeige werden danach bei Ummeldung, soweit sie dadurch unrichtig geworden sind, oder bei Abmeldung des Gewerbes spätestens zehn Jahre nach Ablauf des Jahres, in dem die Um- oder Abmeldung erfolgt ist, gelöscht. Damit wurde einer entsprechenden Forderung von mir Rechnung getragen. Diese Hilfestellung trägt zu einem gleichmäßigen Verwaltungsvollzug bei den Gemeinden als zuständige Gewerbebehörden bei.

2. Elektronische Übermittlung des Anzeigeformulars

Ebenso wie die Muster-Verwaltungsvorschrift wird in den Hinweisen des Bayerischen Staatsministeriums für Wirtschaft, Infrastruktur, Verkehr und Technologie zum Vollzug des Gewerberechts auch der im Rahmen der Novellierung der Gewerbeordnung eingeführten Erleichterung der elektronischen Datenverarbeitung von Gewerbeanzeigen (§ 14 Abs. 4 Satz 3 GewO) Rechnung getragen. So wird dort explizit darauf hingewiesen, dass der Gewerbetreibende das Anzeigeformular auch elektronisch an die Gemeinde übermitteln kann, sofern diese die technischen Voraussetzungen hierfür besitzt. Gleichzeitig wird allerdings klargestellt, dass die Gemeinde nicht verpflichtet ist, die hierfür erforderlichen technischen Vorrichtungen vorzuhalten.

17.2 Änderung des Bewachungsgewerberechts

Am 23.07.2002 trat das Gesetz zur Änderung des Bewachungsgewerberechts in Kraft (BGBl I S. 2724). Die in dem Gesetz enthaltenen Änderungen des § 34 a der Gewerbeordnung und der Bewachungsverordnung dienen dem Ziel, die in der Ge-

werbeordnung und der Bewachungsverordnung geregelten Voraussetzungen für die insbesondere auch im öffentlichen Bereich ausgeführten Tätigkeiten des Bewachungsgewerbes an gestiegene notwendige qualitative Anforderungen anzupassen. Aus datenschutzrechtlicher Sicht sind insbesondere folgende Änderungen relevant:

- In § 8 Abs. 1 der Bewachungsverordnung wird bestimmt, dass die Vorschriften des dritten Abschnitts des Bundesdatenschutzgesetzes (BDSG) nunmehr auch dann Anwendung finden, wenn personenbezogene Daten nicht automatisiert und in unstrukturierter Form erhoben, verarbeitet oder genutzt werden. Durch diese Ausdehnung der Anwendbarkeit des BDSG sollen gerade die vom Sicherheitsgewerbe oftmals benutzten Akten und Aktensammlungen, die keine automatisierten Dateien darstellen, erfasst werden. Dadurch werden die im Zusammenhang mit Bewachungsaufgaben erfassten Informationen aus dem persönlichen Lebensbereich von Betroffenen unabhängig von dem eingesetzten Speichermedium unter einen verstärkten Schutz gestellt.

- Die Neufassung des § 9 Bewachungsverordnung regelt zum einen, dass die Überprüfung der Zuverlässigkeit nunmehr grundsätzlich anhand einer unbeschränkten Auskunft nach § 41 Abs. 1 Nr. 9 Bundeszentralregistergesetz zu beurteilen ist. Daneben können die Gewerbeämter - wie schon zuvor - auch andere Erkenntnisquellen nutzen, insbesondere zusätzliche Auskünfte aus dem Gewerbezentralregister, von der Industrie- und Handelskammer, dem Amtsgericht über Eintragungen nach § 915 ZPO sowie dem Finanzamt einholen. Im neu eingefügten Absatz 2 wird für bestimmte Wachleute außerdem die Möglichkeit einer vertieften Zuverlässigkeitsüberprüfung geschaffen: So kann die zuständige Behörde bei Wachpersonen, die mit Schutzaufgaben von Objekten beauftragt werden sollen, von denen im Falle eines kriminellen Eingriffs eine besondere Gefahr für die Allgemeinheit ausgehen kann, zusätzlich bei der Verfassungsschutzbehörde die Abfrage des nachrichtendienstlichen Informationssystems veranlassen (§ 9 Abs. 2 Satz 2 Bewachungsverordnung). Vor dem Hintergrund der Terroranschläge in den USA soll dadurch gewährleistet werden, dass die Wachleute insbesondere, wenn sie zum Schutz sabotageempfindlicher Bereiche (z.B. Chemieunternehmen oder Lebensmittelherstellungsbetrieb) eingesetzt werden, nicht ihrerseits ein Sicherheitsrisiko darstellen.

- Die mit § 15 BewachV neu eingefügte Regelung soll sicherstellen, dass die Angehörigen des Bewachungsgewerbes über die für diese Branche in besonderem Maße notwendige Zuverlässigkeit nicht nur anfänglich, sondern auch während der gesamten Dauer ihrer Tätigkeit verfügen. Es verbleibt grundsätzlich dabei, dass die Gewerbeämter erst dann in eine erneute Überprüfung der Zuverlässigkeit einsteigen, wenn konkrete Anhaltspunkte vorliegen, wonach die notwendige Zuverlässigkeit nicht mehr gegeben sein könnte. Hierfür kann es verschiedene Erkenntnisquellen (z.B. Presseberichte, Hinweise von Auftraggebern oder anderen Firmen, Beschwerden von Bürgern u.Ä.) geben. Darüber hinaus sollen die Gewerbeämter nun auch automatisch von den Gerichten und Staatsanwaltschaften unterrichtet werden, wenn von dort einschlägige Maßnahmen getroffen werden, die Zweifel an der Eignung oder Zuverlässigkeit hervorrufen können. Inhaltlich hat diese Unterrichtung denselben Informationsgehalt wie ein Führungszeugnis. Von dem Verfahren werden aber nur diejenigen Betroffenen erfasst, bei denen es zu rechtlich relevanten Maßnahmen kommt.

Das Bayerische Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie hat im Zuge der Deregulierung auch hier auf die Novellierung der Allgemeinen Verwaltungsvorschrift zum § 34 a der Gewerbeordnung und zur Bewachungsverordnung (BewachVwV) verzichtet. An Stelle dessen wurden mit Schreiben vom 4.12.2003 sog. Hinweise zum Vollzug des Bewachungsgewerberechts als Arbeitshilfe erstellt, bei deren Erstellung ich beteiligt wurde.

18 Statistik

18.1 Forschungsdatenzentrum der Statistischen Landesämter

Eine vom Bundesministerium für Bildung und Forschung eingesetzte Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik hat in einem Gutachten vom März 2001 die Einrichtung von sog. „Forschungsdatenzentren“ empfohlen, um der Wissenschaft eine verbesserte Nutzung von Daten der amtlichen Statistik zu ermöglichen. Das Statistische Bundesamt hat daraufhin für seinen Zuständigkeitsbereich ein derartiges Forschungszentrum gegründet. Die weit überwiegende Mehrzahl der Daten, aus denen Bundesstatistiken erstellt werden, befindet sich allerdings im Verfügungsbereich der Statistischen Ämter der Länder. Diese haben das ausschließliche Zugriffsrecht auf die

von Ihnen erhobenen Einzelangaben. Die Statistischen Ämter der Länder haben dementsprechend ebenfalls ein Forschungsdatenzentrum (FDZ) gegründet. Das FDZ wird von einem Lenkungsausschuss geleitet, dessen Vorsitz zurzeit beim Präsidenten des Bayerischen Landesamtes für Statistik und Datenverarbeitung liegt. Ich wurde frühzeitig in die Planungen eingeschaltet.

Die Planungen für das FDZ sahen ursprünglich im Wesentlichen vor:

- den Aufbau und den Betrieb eines Servernetzes für eine fachlich zentralisierte Datenbereitstellung,
- die Entwicklung und die Pflege eines dazugehörigen Metadateninformationssystems,
- die Einrichtung und den Betrieb von Arbeitsplätzen für Gastwissenschaftler (sog. „one-dollar-men“) mit der Möglichkeit des Zugriffs auf nicht anonymisierte Daten,
- die Einrichtung und den Betrieb einer kontrollierten Datenfernverarbeitung sowie
- die Gewährleistung der Betreuung und Beratung der Nutzer.

Weiterhin waren die Durchführung von Forschungsprojekten zur Erstellung von Scientific-Use-Files (faktisch anonymisierte Mikrodaten) und Public-Use-Files (absolut anonymisierte Mikrodaten) sowie die Durchführung von Projekten zur methodisch-inhaltlichen Weiterentwicklung der angewandten amtlichen Statistik zusammen mit dem Statistischen Bundesamt vorgesehen.

Aus datenschutzrechtlicher Sicht waren insbesondere die fachlich zentralisierte Datenbereitstellung, die Einrichtung und der Betrieb einer kontrollierten Datenfernverarbeitung und die Einrichtung und der Betrieb von Gastwissenschaftlerarbeitsplätzen klärungsbedürftig.

1. Die Bestimmungen des § 16 Bundesstatistikgesetz (BStatG) bzw. der Art. 17, 18 Bayerisches Statistikgesetz (BayStatG) regeln die statistische Geheimhaltung und die Zweckbindung von Einzelangaben. Danach sind Einzelangaben in der Regel geheim zu halten. Sie dürfen grundsätzlich ausschließlich für statistische Zwecke verarbeitet oder genutzt werden. Für die Durchführung wissenschaftlicher Arbeiten enthalten allerdings § 16 Abs. 6 BStatG bzw. Art. 18 Abs. 5 BayStatG Öffnungsklauseln. Danach ist eine Übermittlung von Einzelangaben dann zulässig, wenn die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können (faktische Anonymisierung). Selbst dann sehen § 16 Abs. 7 BStatG sowie Art. 18 Abs. 5 Sätze 2 und 3 BayStatG die Verpflichtung der Empfänger nach dem Verpflichtungsgesetz vor. Bei dem mir vorgestellten Verfahren der Gastwissenschaftlerarbeitsplätze („one-dollar men“) im FDZ bin ich davon ausgegangen, dass die Gastwissenschaftler in einer Vielzahl von Fällen Einblick in statistisches Datenmaterial erhalten, das die genannten Anforderungen an eine (faktische) Anonymisierung nicht erfüllt. Ich habe deshalb in dem angedachten Institut der Gastwissenschaftlerarbeitsplätze eine Umgehung der Bestimmungen des § 16 Abs. 6 BStatG bzw. des Art. 18 Abs. 5 BayStatG gesehen.

   Das FDZ hat von der Einrichtung derartiger Gastwissenschaftlerarbeitsplätze inzwischen Abstand genommen.

2. Im Rahmen der kontrollierten Datenfernverarbeitung erstellen Wissenschaftler zu ihren Forschungsvorhaben ein Auswertungsprogramm. Betroffene Standorte des FDZ prüfen das Programm, lassen es mit den benötigten Mikrodaten ablaufen und führen eine Auswertung durch. Die Wissenschaftler haben somit keinen direkten Kontakt mit den geheimhaltungsbedürftigen Mikrodaten; eine Anonymisierung der Mikrodaten muss daher nicht vorgenommen werden. Die Ergebnisse werden vor Auslieferung an die Wissenschaftler auf Wahrung der Geheimhaltung geprüft. Die Wissenschaftler erhalten nur Datenmaterial, das den Vorschriften der statistischen Geheimhaltung genügt.

   Gegen dieses Verfahren habe ich keine datenschutzrechtlichen Einwendungen erhoben.

3. Von entscheidender Bedeutung für die datenschutzrechtliche Beurteilung des FDZ ist die rechtliche Einordnung der fachlich zentralisierten Datenbereitstellung an einem Standort des FDZ als Datenverarbeitung im Auftrag oder als Funktionsübertragung. Grundsätzlich ist zu bemerken, dass auch bei einer fachlich zentralisierten Datenbereitstellung ausschließlich faktisch anonymisierte Mikrodaten i.S. des § 16 Abs. 6 BStatG bzw. Art. 18 Abs. 5 BayStatG den Bereich der Statistik verlassen dürfen. Dies wurde von Seiten des FDZ auch zugesichert.

   Die Bereitstellung von faktisch anonymisierten Mikrodaten für die Wissenschaft ist zwar keine Standardaufgabe der Statistischen Landesämter. Andererseits schreibt § 1 BStatG

ausdrücklich die Dienstleistungsfunktion der amtlichen Statistik fest. Diese umfasst die Verpflichtung, die Daten der amtlichen Statistik - auch der Wissenschaft - als öffentliches Gut bereitzustellen. So wurden bereits in der Vergangenheit bei länderübergreifenden Datenanfragen für ein konkretes Forschungsvorhaben die benötigten Daten einem koordinierenden Landesamt zur Auswertung zur Verfügung gestellt. Dabei handelt es sich jedoch um ein zeit- und kostenintensives Verfahren, das durch den Aufbau einer fachlich zentralisierten Datenbereitstellung im Rahmen des FDZ überflüssig werden soll.

Nach den mir vorgelegten Unterlagen sind die Statistischen Landesämter, bei denen Daten fachlich zentralisiert vorgehalten werden sollen (sog. Serverämter), nicht befugt, eigenständig über Nutzungsanfragen zu entscheiden. Die Serverämter dürfen die Daten vielmehr nur im Rahmen der Weisungen und vertraglichen Vorgaben des Eigneramts verarbeiten. Diese Weisungen werden schriftlich erteilt. Jede Verarbeitung der Daten wird automatisch protokolliert, um dem Eigneramt die Möglichkeit zu geben, die auftragsgemäße Datenverarbeitung zu kontrollieren. Die Daten werden nur dem im FDZ zuständigen Personal zugänglich gemacht. Die Verantwortung für die Datenverarbeitung liegt daher weiterhin beim Eigneramt.

Bei den genannten Vorgaben habe ich es als vertretbar angesehen, zumindest während einer zeitlich abgegrenzten Pilotierungsphase von einer Datenverarbeitung im Auftrag auszugehen. Langfristig sollte das FDZ allerdings auf eine eigenständige Rechtsgrundlage gestellt werden.

In mehreren Sitzungen der Arbeitskreise Statistik und Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder wurde - bei Stimmenthaltung meinerseits und einer Gegenstimme - ein Papier erarbeitet, das im Grundsatz bereits für den Testbetrieb eine Rechtsgrundlage fordert und nur unter starker regionaler und zeitlicher Beschränkung einen Pilotbetrieb des FDZ als tolerabel erachtet. Mit maßgebend dafür war die Auffassung, dass das Bundesstatistikgesetz im Gegensatz zu den Landesstatistikgesetzen eine Datenverarbeitung im Auftrag nicht kenne. Diese Auffassung ist aber in der Lehre umstritten, ich teile sie ebenfalls nicht. Auch aus diesem Grund ist es meiner Meinung nach notwendig, hier zu einer gesetzlichen Klarstellung zu kommen.

Der Vorsitzende des Lenkungsausschusses des FDZ hat mir inzwischen mitgeteilt, dass im Rahmen derzeit erarbeiteter Änderungen statistischer Rechtsgrundlagen auch eine Anpassung des Bundesstatistikgesetzes vorgesehen ist, die u.a. die Übermittlung von Mikrodaten zwischen den Statistischen Landesämtern sowie die Bereitstellung von Daten für die Wissenschaft regeln soll.

19 Landwirtschaft

19.1 Übermittlung von Viehbestandsdaten durch die Tierseuchenkasse an Gemeinden

Bis zum 31.12.2003 war es gesetzliche Aufgabe der Gemeinden, die Beiträge zur Bayerischen Tierseuchenkasse von den Tierhaltern zu erheben. Zur Vereinfachung und Beschleunigung der Verwaltungsverfahren wurde diese Aufgabe im Zuge der Verwaltungsreform ab 01.01.2004 auf die Tierseuchenkasse übertragen.

Die Tierbestandsdaten werden nunmehr von der Tierseuchenkasse selbst erhoben. Damit fallen diese Daten bei den Gemeinden nicht mehr an. Zahlreiche gemeindliche Gebührensatzungen sehen jedoch – abhängig von Art und Umfang des Tierbestandes – einen Abschlag auf die gemeindlichen Kanalbenutzungsgebühren vor. Eine Gemeinde fragte daher bei mir an, ob die Übermittlung der aktuellen Viehbestandsdaten durch die Tierseuchenkasse an die Gemeinden zur Berechnung der Kanalbenutzungsgebühren datenschutzrechtlich zulässig ist. Ich habe ihr Folgendes mitgeteilt:

Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind grundsätzlich beim Betroffenen, also dem jeweiligen Tierhalter, mit seiner Kenntnis zu erheben (Art. 16 Abs. 2 Satz 1 BayDSG). Nur in eng umrissenen Ausnahmefällen dürfen personenbezogene Daten bei Dritten, hier also bei der Tierseuchenkasse, erhoben werden (Art. 16 Abs. 2 Satz 2 BayDSG). Ein solcher Ausnahmefall liegt hier nicht vor. Insbesondere kommt eine Datenübermittlung zwischen öffentlichen Stellen gemäß Art. 16 Abs. 2 Satz 2 Nr. 3 i.V.m. Art. 18 Abs. 1, Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG nicht in Betracht, da die Daten von der Tierseuchenkasse nicht zum Zweck der Berechnung der Kanalbenutzungsgebühren erhoben wurden und auch keine Rechtsvorschrift existiert, die die Nutzung der von der Tierseuchenkasse erhobenen Daten für diesen Zweck vorsieht.

Mithin darf die Gemeinde die zur Berechnung der Kanalbenutzungsgebühren notwendigen Angaben nur bei den betroffenen Tierhaltern selbst erheben. Allerdings wäre es zur Verwaltungsvereinfa-

chung beispielsweise datenschutzrechtlich zulässig, dass die Gemeinde die in ihrem Gebiet ansässigen Tierhalter - ggf. durch ortsübliche Bekanntmachung - zur Einreichung der entsprechenden Unterlagen innerhalb einer angemessenen Frist auffordert.

20 Schulen und Hochschulen

20.1 Schulen

20.1.1 Information der früheren Erziehungsberechtigten volljähriger Schüler

Bereits in Nr. 16.1.1 meines letzten Tätigkeitsberichts habe ich mich mit den zu Beginn des Schuljahres 2002/2003 in Kraft getretenen Bestimmungen der Art. 88 a und Art. 75 Abs. 1 Satz 2 BayEUG befasst, nach denen frühere Erziehungsberechtigte volljähriger Schüler, welche das 21. Lebensjahr noch nicht vollendet haben, über schwere Ordnungsmaßnahmen nach Art. 86 Abs. 2 Satz 1 Nr. 3 bis 10 BayEUG (Versetzung in eine andere Klasse bis Ausschluss von allen Schulen auch mehrerer Schularten) sowie über ein auffallendes Absinken des Leistungsstands und sonstige wesentliche, den Schüler betreffende Vorgänge unterrichtet werden sollen. Schon damals habe ich ausgeführt, dass in die Auslegung dieser Soll-Bestimmungen z.B. auch pädagogische Überlegungen (besondere Situation in der Familie etc.) einfließen können, die gegen eine Information in diesen Fällen sprechen. Für selbstverständlich habe ich es erachtet, dass der Schüler oder die Schülerin von der Absicht, die Eltern zu verständigen, unterrichtet wird.

Ich habe mich deshalb beim Staatsministerium für Unterricht und Kultus dafür eingesetzt, dass die Schulen dazu angehalten werden, im Regelfall den Schüler oder die Schülerin vor einer Benachrichtigung der früheren Erziehungsberechtigten zu informieren. In Anbetracht des Grundrechts auf informationelle Selbstbestimmung gem. Art. 100 i.V.m. Art. 101 BV ist es meiner Meinung nach erforderlich, dass der Schüler oder die Schülerin Gelegenheit erhält, Gründe vorzutragen, die im Einzelfall gegen eine Information der Eltern sprechen und dass die Schule diese in ihre Entscheidung einbeziehen kann. Das Kultusministerium hat das ursprünglich nicht für notwendig gehalten.

Nachdem ich mich persönlich an den Amtschef des Kultusministeriums gewandt hatte, hat dieser mit Schreiben vom 08.10.2003, Az.: III.1-5S4600-6.72 901, alle Hauptschulen, Förderschulen, Realschulen, Gymnasien und beruflichen Schulen darauf hingewiesen, dass **vor einer Benachrichtigung der früheren Erziehungsberechtigten der volljährige Schüler im Regelfall zu informieren sei**. Trage der Schüler gegen eine Unterrichtung seiner früheren Erziehungsberechtigten Gründe vor, seien diese bei der Entscheidung über die Information der früheren Erziehungsberechtigten zu würdigen. Im Ausnahmefall sei von deren Unterrichtung abzusehen. Ein Verzicht auf die Mitteilung könne z.B. geboten sein, wenn dem Schüler schwer wiegende häusliche Auseinandersetzungen drohen oder er zu seinen früheren Erziehungsberechtigten keinen Kontakt mehr hat. Überdies wird den Schulen empfohlen, die Information des volljährigen Schülers und die Information der früheren Erziehungsberechtigten aktenkundig zu machen.

Am 30.09.2004 hat der **Bayerische Verfassungsgerichtshof** festgestellt, dass die Art. 75 Abs. 1 Satz 2 und Art. 88 a BayEUG mit der Bayerischen Verfassung, vor allem den Grundrechten aus Art. 100, 101 BV und dem darin enthaltenen Recht auf informationelle Selbstbestimmung vereinbar seien. Die Einbeziehung der früheren Erziehungsberechtigten bedürfe wegen des Rechts auf informationelle Selbstbestimmung der Schülerinnen und Schüler allerdings einer verfahrensmäßigen Absicherung, um eine Unterrichtung der Eltern in den Fällen zu verhindern, in denen sie nicht angebracht und damit unverhältnismäßig ist. Der betroffene Schüler müsse daher Gelegenheit haben, sich - in der Regel vor der Unterrichtung seiner früheren Erziehungsberechtigten - zu äußern. Eine derartige verfahrensmäßige Absicherung der Rechte des betroffenen Schülers könne den angegriffenen Regelungen im Wege der Auslegung entnommen werden. In diesem Zusammenhang hat der Verfassungsgerichtshof des Weiteren ausgeführt:

„..... Die Schule kann diese Aufgabe nur dann in einer sachgerechten, den verfassungsrechtlichen Grundsätzen gerecht werdenden Weise erfüllen, wenn sie vor einer Entscheidung über die Unterrichtung der früheren Erziehungsberechtigten dem betroffenen Schüler Gelegenheit gibt, seine persönliche Situation darzulegen, besonders seine Lebensumstände, sein Verhältnis zu seinen früheren Erziehungsberechtigten und sonstige, ihm im Zusammenhang mit dem Anlass der eventuellen Unterrichtung wichtig erscheinende Gesichtspunkte. ..... Der Vollzugshinweis des Bayerischen Staatsministeriums für Unterricht und Kultus vom 08.10.2003 zeigt, dass auch in der Praxis von der Notwendigkeit zum vorgängigen Gespräch mit dem betroffenen Schüler ausgegangen wird. .....“

Das Gericht hat damit den von mir erreichten Vollzugshinweis als wesentlichen Grund für die Annahme der Verfassungsmäßigkeit der angegriffenen Regelungen angesehen.

20.1.2 Sicherheitskonzept an Schulen

Vor dem Hintergrund des „Amoklaufs von Erfurt“ hat das Staatsministerium für Unterricht und Kultus im Frühjahr 2002 die Schulen gebeten, in Zusammenarbeit mit Schulamt, Eltern, Sachaufwandsträgern, Gemeinde, Polizei, Feuerwehr, Rettungsdiensten und ggf. Jugendämtern jeweils ein örtliches **Sicherheitskonzept** zu entwickeln. Als Hilfestellung für die Schulen hat eine Arbeitsgruppe aus Vertretern des Kultus- und des Innenministeriums Anregungen und Empfehlungen für die Erstellung eines solchen Konzepts erarbeitet. Damit sollte den Schulen eine Orientierungshilfe für die flexible Umsetzung sowie für die beständige Fortschreibung und Aktualisierung an die Hand gegeben werden (siehe dazu das KMS vom 18.11.2002, Az.: III-S4313-6/104947).

Leider wurde ich in die Erarbeitung dieses Konzepts nicht eingeschaltet. Erst durch Anfragen zahlreicher Schulen, die sich wegen Problemen im Bereich des Datenschutzes (z.B. bei der Datenübermittlung an die Polizei und bei der Hinterlegung von Daten bei Kommunen) an mich wandten, wurde ich auf die Orientierungshilfe aufmerksam. Im Rahmen meiner Überprüfung stellte ich fest, dass im Konzept die notwendigen detaillierten Ausführungen zur datenschutzrechtlichen Problematik fehlten. Ich habe deshalb das Kultusministerium gebeten, mich künftig über derartige weit reichende Maßnahmen frühzeitig zu unterrichten und hinsichtlich der datenschutzrechtlichen Thematik zu beteiligen.

In der Folgezeit erreichte ich eine Klärung der von den Schulen aufgebrachten Fragen. Entsprechend hat das Kultusministerium mit KMS vom 07.10.2003, Az.: III-5S4312.2-6.111578, alle Schulen über die „Übermittlung und Hinterlegung von Daten durch die Schulen“ informiert.

Datenübermittlung

Gemäß Art. 85 Abs. 2 Satz 1 BayEUG ist die Weitergabe von Daten und Unterlagen über Schüler und Erziehungsberechtigte an außerschulische Stellen untersagt, falls nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird. Nach Art. 42 PAG besteht dieser rechtliche Anspruch, sofern die Datenübermittlung zur Erfüllung der polizeilichen Aufgaben erforderlich ist. Dies ist jeweils **im Einzelfall** zu prüfen. Häufig stellt sich die Frage des rechtlichen Anspruchs z.B. bei von der Schule ausgeschlossenen (oder im Zuge einer Ordnungsmaßnahme entlassenen) Schülern. Dabei lassen sich folgende Fallgruppen unterscheiden:

1. Wird ein „Problemschüler“ aus disziplinarischen Gründen entlassen oder ausgeschlossen, weil er gegenüber seinen Mitschülern oder Lehrern bereits gewalttätig in Erscheinung getreten ist, und lässt die Entfernung aus der Schule „Rachefeldzüge“ gegen Lehrkräfte oder Schüler und/oder ein Abgleiten in die Kriminalität befürchten, kann die Erforderlichkeit bei einem nicht mehr der Schulpflicht unterliegenden Schüler zweifellos bejaht werden (schulpflichtige Schüler müssen ggf. eine andere Schule besuchen).

2. Muss dagegen ein Schüler die Schule z.B. nur deshalb verlassen, weil er die Leistungsanforderungen nicht erfüllt (und wechselt auf eine Schule einer anderen Schulart), ist die Erforderlichkeit zu verneinen, soweit keine zusätzlichen Anhaltspunkte dafür bestehen, dass der Schüler wegen des Verlassens der Schule zu einer Gefahr für die öffentliche Sicherheit und Ordnung werden könnte.

Demnach sind die entsprechenden Daten zum Schutz potenzieller Opfer, aber auch im Hinblick darauf, ein eventuelles Abgleiten eines „ausgeschlossenen“ Schülers in die Kriminalität zu verhindern, dann herauszugeben, wenn es sich um „polizeilich relevante“ Schulausschlüsse im Sinn der 1. Fallgruppe handelt.

Im Übrigen ergibt sich aus Art. 85 BayEUG sowie aus Art. 42 PAG, dass eine **Datenübermittlung „auf Vorrat“**, bei der Schulen zur Sicherstellung der telefonischen Erreichbarkeit Telefonnummern der Erziehungsberechtigten aller Schüler - womöglich noch regelmäßig zu bestimmten Zeitpunkten im Jahr - an die örtliche Polizeidienststelle übermitteln, **nicht zulässig** ist, da diese Daten zur Erfüllung der polizeilichen Aufgaben nicht erforderlich sind.

Die Weitergabe der Daten des „Verantwortlichen“ der Schule ist dagegen anders zu beurteilen; solche Angaben (z.B. Schulleiter) werden in der Regel auch anderweitig veröffentlicht, sodass eine derartige Übermittlung keine Beeinträchtigung des Persönlichkeitsrechts des „Verantwortlichen“ der Schule darstellt.

Hinterlegung von Adressdaten

Bei einer offenen Hinterlegung von Adressdaten würde es sich um eine Datenübermittlung handeln, die – wie oben bemerkt – unzulässig wäre. Daher sollen die Adressdaten bei der Kommune, bei einem Mitarbeiter der Schulleitung und ggf. bei Polizei oder Feuerwehr nur verschlossen hinterlegt werden. Herr der Daten bleibt weiterhin die Schule; nur sie übt das Zugriffsrecht aus. Meiner Ansicht nach müssen die Daten daher im Rahmen einer „Containerlösung“ oder „versiegelt“ hinterlegt werden. Dabei haben die Schulen Vorkehrungen zu treffen, dass die hinterleg-

ten Daten wirklich nur im Notfall und dann auch nur mit Genehmigung der Schule verwendet werden können. Ist dies gewährleistet, so spricht auch nichts gegen eine Hinterlegung von Daten, sei es in Form von Listen auf Papier oder auf CD gebrannt.

Die Hinterlegung der Daten sollte aber auf zwei Stellen beschränkt bleiben. Dabei ist einem Mitarbeiter der Schulleitung und der Kommune der Vorrang einzuräumen. Eine Hinterlegung bei Feuerwehr oder Polizei sollte nur in praxisbedingten Ausnahmefällen erfolgen.

20.1.3 Veröffentlichung von Schülerfotos

Obgleich ich mich bereits in Nr. 15.1 meines 19. Tätigkeitsberichts mit dieser Thematik befasst habe und zwischenzeitlich die „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes (KMBek vom 19.04.2001, KWMBl I S. 112, geändert durch KMBek vom 10.10.2002, KWMBl I S. 354) unter Nr. 4.4 in den Buchstaben d (Herausgabe eines Jahresberichts für die Schüler und Erziehungsberechtigten der Schule - Art. 85 Abs. 3 BayEUG) und e (Öffentlichkeitsarbeit der Schule - Art. 57 Abs. 3 BayEUG) diesbezügliche Regelungen enthalten, erreichen mich immer wieder Anfragen zur Veröffentlichung von Schülerfotos, weil die Schulen diese Vorgaben nicht beachten. Beispielsweise haben die Schulen diejenigen Schüler, die bzw. deren Erziehungsberechtigte mit einer Veröffentlichung des Klassenfotos im Internet nicht einverstanden waren, dazu aufgefordert, von der Aufnahme des Fotos fernzubleiben. Dadurch werden Kinder, deren Fotos nicht im Internet veröffentlicht werden sollen, von Klassenfotos ausgeschlossen und damit ausgegrenzt, was mit dem Sinn und Zweck des Datenschutzes (vgl. Art. 1 BayDSG) nicht vereinbar ist.

Veröffentlichungen von Schülerfotos auf der Homepage einer Schule, im Jahresbericht oder auch in der (lokalen) Presse sind datenschutzrechtlich als Datenübermittlungen an Dritte einzustufen, die **nur mit Einwilligung der Betroffenen** zulässig sind. Dies gilt auch dann, wenn den Fotos keine Namensangaben beigefügt sind.

Angesichts des engen Adressatenkreises eines gedruckten **Jahresberichts** sehe ich es hier als ausreichend an, wenn die Betroffenen zu Beginn eines jeden Schuljahres hinreichend deutlich darüber informiert werden, dass Fotos in den Jahresbericht aufgenommen werden sollen, und ihnen die Möglichkeit eines Widerspruchs eingeräumt wird. Sofern nur einzelne auf einem Foto abgebildete Personen von ihrem Widerspruchsrecht Gebrauch machen, können diese dann in geeigneter Form unkenntlich gemacht werden.

In den **übrigen Fällen** kann auf eine ausdrückliche Einwilligung der Betroffenen, die vorher auch über die besonderen Risiken einer solchen Veröffentlichung zu informieren sind, nicht verzichtet werden (vgl. Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG). Zur Einholung der Einwilligung habe ich mich in dem eingangs erwähnten Tätigkeitsbericht dergestalt geäußert, dass sie so zu erfolgen hat, dass sich die Betroffenen nicht einem Gruppendruck ausgesetzt fühlen. Sollen Schülerfotos im **Internet** veröffentlicht werden, sind die Betroffenen auch darauf hinzuweisen, dass sich ins Internet eingestellte Daten in der Regel problemlos auslesen lassen und damit nachteilige Auswirkungen verbunden sein können. Dieser Hinweis wurde auch in die Nr. 4.4 Buchstabe e der o.g. „Erläuternden Hinweise“ aufgenommen. Aus gegebenem Anlass weise ich ergänzend darauf hin, dass pauschale Einverständniserklärungen, z.B. beim Schuleintritt, nicht ausreichend sind.

Da ich feststellen musste, dass nicht nur einzelne Schulen diese Vorgaben missachten, habe ich das Staatsministerium für Unterricht und Kultus erneut eingeschaltet. Das Kultusministerium will im Rahmen der regelmäßigen Dienstbesprechungen mit den Schulaufsichtsbehörden an den Datenschutz bei der Aufnahme von Klassenfotos erinnern. Die Schulen sollen insbesondere dazu angehalten werden, auch bei Klassenfotos keinen unangemessenen Gruppendruck gegenüber denjenigen Schülern aufzubauen, die nicht mit dem Klassenfoto im Internet veröffentlicht werden wollen. Ihnen werden vom Kultusministerium nunmehr folgende Vorgehensweisen empfohlen:

1. Klassenfotos, die sowohl für die Veröffentlichung im gedruckten Jahresbericht als auch auf der Schulhomepage vorgehen sind, können zwei Mal aufgenommen werden. Eine der Aufnahmen ist für den Abdruck im Jahresbericht bestimmt - wobei ich darauf hinweise, dass auch hier Fotos der Einwilligung bedürfen, vgl. Nr. 4.4 Buchstabe d der „Erläuternden Hinweise“ -, die andere Aufnahme für die Veröffentlichung auf der Schulhomepage. Die nicht mit ihrer Veröffentlichung im Internet einverstandenen Schüler (bzw. Schüler, bei denen die erforderliche Einwilligung ihrer Erziehungsberechtigten nicht vorliegt) sollen bei der für das Internet bestimmten Aufnahme Gelegenheit erhalten, beiseite zu treten.

2. Schulen können Klassenfotos vor der Einstellung ins Internet mit Hilfe von geeigneter Software so bearbeiten, dass diejenigen Schüler in der Aufnahme unkenntlich gemacht

werden, deren Einwilligung zur Internetveröffentlichung nicht vorliegt.

Diese Hinweise erachte ich für zielführend.

20.1.4 Nutzung der EDV-Einrichtungen an den Münchener Schulen

Mehrere Münchener Schüler machten mich darauf aufmerksam, dass die Rechtsabteilung des Schul- und Kultusreferats der Landeshauptstadt München eine „Nutzungsordnung der EDV-Einrichtungen an der Schule“ erstellt hat, die den Schülern bzw. deren Erziehungsberechtigten zur Unterschrift vorgelegt worden ist. In einer dieser Nutzungsordnung angefügten Erklärung soll durch Unterschrift anerkannt werden, dass die Schule den Datenverkehr protokolliert, zeitlich begrenzt speichert und auch Stichproben vornimmt. Ferner sollen sich die Schüler bzw. die Erziehungsberechtigten damit einverstanden erklären, dass eine Einsichtnahme in verschickte und empfangene E-Mails stichprobenartig oder im Einzelfall erfolgen kann. In diesen Klauseln haben die betroffenen Schüler eine Verletzung datenschutzrechtlicher Vorschriften gesehen.

Angesichts der Beschränkung der Nutzung nur für schulische Zwecke sehe ich keinen Verstoß gegen datenschutzrechtliche Vorschriften.

Zur Überprüfung der Angelegenheit habe ich sowohl eine Stellungnahme des Schul- und Kultusreferats der Landeshauptstadt München als auch des Staatsministeriums für Unterricht und Kultus eingeholt. Angesichts der Tatsache, dass der Schule, insbesondere den verantwortlichen Lehrkräften, eine Kontroll- und Aufsichtspflicht gegenüber den Schülern obliegt, bin ich zu folgender datenschutzrechtlichen Bewertung gekommen:

Bei den **städtischen Schulen** dürfen gemäß der Nutzungsordnung die zur Verfügung gestellten EDV-Einrichtungen **nur für schulische Zwecke** genutzt werden. Insofern sind die Schulen nicht geschäftsmäßige Erbringer von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (§ 3 Nr. 10 TKG) und damit auch nicht auf das Fernmeldegeheimnis nach § 88 TKG verpflichtet.

Das Kultusministerium hat beschlossen, die Nutzungsordnung für die städtischen Schulen auch für die **staatlichen Schulen** verbindlich machen zu lassen. Damit dürfen auch die bei den staatlichen Schulen zur Verfügung gestellten EDV-Einrichtungen **nur für schulische Zwecke** genutzt werden. Demgemäß sind auch die staatlichen Schulen nicht dem in § 88 TKG normierten Fernmeldegeheimnis unterworfen.

Aufgrund des Verbots der privaten Nutzung der zur Verfügung gestellten EDV-Einrichtungen sind die Protokollierung des Datenverkehrs, dessen begrenzte zeitliche Speicherung und das Vornehmen von Stichproben (auch beim E-Mail-Verkehr) durch die Schule datenschutzrechtlich zulässig. Die geforderte Einverständniserklärung begegnet damit keinen datenschutzrechtlichen Bedenken. Einen Verstoß gegen datenschutzrechtliche Vorschriften konnte ich daher nicht feststellen.

Diese Auffassung steht mit Abschnitt II Buchstabe h der Orientierungshilfe des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (diese ist auf meiner Homepage unter www.datenschutz-bayern.de/verwaltung/63OHinternd.pdf abrufbar) in Einklang. Danach darf nämlich der Dienstherr bzw. Arbeitgeber im Fall der ausschließlich für dienstliche Zwecke zugelassenen Nutzung von ein- und ausgehenden E-Mails seiner Beschäftigten im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. So könnte der Vorgesetzte beispielsweise verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.

An dieser Stelle weise ich darauf hin, dass die „Rechtlichen Hinweise zur Nutzung des Internets an Schulen“ mitsamt dem „Muster für eine Nutzungsordnung der Computereinrichtungen an Schulen“ (www.datenschutz.hessen.de/o-hilfen/AnlageA.htm und www.datenschutz.hessen.de/o-hilfen/AnlageB.htm) dringend der Überarbeitung durch die Kultusministerkonferenz bedürfen. Sie widersprechen nämlich den datenschutzrechtlichen Vorschriften einzelner Länder, so auch denen des Freistaates Bayern. In dieser Angelegenheit werde ich auf das Kultusministerium zugehen.

20.1.5 Übermittlung von Zensuren und Abschlusszeugnissen durch Schulen an Firmen

Ein Absolvent einer Fachschule hat mir vorgetragen, dass die Schule ein Notenblatt mit seinen Zensuren und sein Abschlusszeugnis ohne seine Einwilligung an seinen Arbeitgeber in Kopie übermittelt habe.

In ihrer Stellungnahme hat die betroffene Fachschule ausgeführt, dass die Ausbildung der Schülerinnen und Schüler von einer namhaften Firma in besonderem Maße unterstützt werde. Daher sei die Firma an einer leistungs- und zielorientierten Ausbildung ihrer Mitarbeiter als Fachschüler interessiert. Aus diesem Grund hätten sich die Fachschüler vertraglich gegenüber der Firma verpflichtet, jederzeit Auskunft über

den schulischen Leistungsstand zu geben. Aus Vereinfachungsgründen würden nun die Noten und Abschlusszeugnisse direkt von der Fachschule der Firma zugeleitet.

Die Übermittlung von Zensuren und Abschlusszeugnissen durch Schulen an Firmen ohne Einwilligung der Schülerinnen und Schüler ist datenschutzrechtlich unzulässig.

Nach der datenschutzrechtlichen Sonderregelung des Art. 85 Abs. 1 Satz 1 BayEUG sind die Erhebung und die Verarbeitung (dazu zählt auch die Übermittlung) von Daten nur zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben zulässig. Im Übrigen ist die Weitergabe von Daten und Unterlagen über Schüler und Erziehungsberechtigte an außerschulische Stellen gem. Art. 85 Abs. 2 Satz 1 BayEUG untersagt, falls „nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird".

Da die Übermittlung von Zensuren und Abschlusszeugnissen durch Schulen an Firmen weder der Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben dient noch (im Regelfall) ein rechtlicher Anspruch der Firmen auf die Herausgabe dieser Daten besteht, ist sie nach Art. 85 BayEUG nicht zulässig.

Nach Art. 2 Abs. 7 BayDSG geht die die Datenübermittlung an außerschulische Stellen regelnde Norm des Art. 85 Abs. 2 BayEUG den Vorschriften des BayDSG über die Datenübermittlung innerhalb des öffentlichen Bereichs (Art. 18 BayDSG) und an Stellen außerhalb des öffentlichen Bereichs (Art. 19 BayDSG) vor. Hinsichtlich der Übermittlung von Zensuren und Abschlusszeugnissen durch Schulen an Firmen ist daher ein Rückgriff auf Art. 19 BayDSG nicht möglich.

Schließlich kann - unabhängig von der Frage, ob eine Einwilligung im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG im Bereich des Art. 85 Abs. 2 BayDSG überhaupt Platz greifen kann - eine datenschutzrechtlich beachtliche Einwilligung jedenfalls nicht auf eine vertragliche Verpflichtung zwischen einem Schüler und der Auskunft ersuchenden Firma gestützt werden. Wie sich aus Art. 15 Abs. 2 BayDSG ergibt, muss nämlich die Einwilligung von der datenverarbeitenden Stelle selbst, hier also von der Schule, beim Betroffenen, d.h. beim Schüler, eingeholt werden. Zudem sind die von den Art. 15 Abs. 2 bis 4 BayDSG aufgestellten formellen Anforderungen (Hinweispflichten, Schriftform etc.) von der die Einwilligung einholenden Stelle einzuhalten.

Ich habe das Staatsministerium für Unterricht und Kultus aufgefordert, die betroffenen Schulen auf diese Rechtslage aufmerksam zu machen.

20.2 Hochschulen

20.2.1 Studentische Evaluation von Lehrveranstaltungen

Obwohl ich mich bereits grundlegend in Nr. 15.4 meines 19. Tätigkeitsberichts zur Evaluation der Lehre an bayerischen Hochschulen geäußert habe, haben mich im Berichtszeitraum zahlreiche weitere Anfragen zur Auslegung des Art. 39 a BayHSchG erreicht. Dabei ging es immer wieder um die Fragen, welche Angaben in den Lehrbericht aufgenommen werden dürfen und wem die Ergebnisse der studentischen Befragungen zur Verfügung gestellt werden dürfen. Ich wurde auch um Beurteilung der Frage gebeten, ob eine Veröffentlichung der Evaluationsergebnisse mit Einwilligung der akademischen Lehrkräfte zulässig ist.

Zum Lehrbericht und zur Auswertung der studentischen Evaluationen weise ich aus datenschutzrechtlicher Sicht auf Folgendes hin:

- Nach Art. 39 a Abs. 2 Satz 4 Halbsatz 2 BayHSchG erstattet der Studiendekan jährlich dem Fachbereichsrat einen Bericht zur Lehre (Lehrbericht). Der **Lehrbericht** enthält gem. Art. 39 a Abs. 3 Satz 1 Halbsatz 2 BayHSchG für den Berichtszeitraum auch Angaben über die Bewertung des Lehrangebots in den einzelnen Studiengängen durch die Studenten. Da die **Veröffentlichung** des Lehrberichts keiner Beschränkung unterliegt, dürfen studentische Bewertungen allerdings nicht unter Angabe der Bezeichnung der Lehrveranstaltungen und der Namen der Lehrenden dargestellt werden.

- Die Bezeichnung der Lehrveranstaltungen, die Namen der Lehrenden und die ausgewerteten **Ergebnisse der studentischen Befragungen** werden nach Art. 39 a Abs. 3 Satz 4 Halbsatz 1 BayHSchG **nur dem Fachbereichsrat und der Leitung der Hochschule** bekannt gegeben und zur Bewertung der Lehre verwendet; vor der Bekanntgabe an den Fachbereichsrat und die Leitung der Hochschule ist den betroffenen Lehrenden gemäß Art. 39 a Abs. 3 Satz 4 Halbsatz 2 BayHSchG Gelegenheit zur schriftlichen Stellungnahme zu den Bewertungsergebnissen zu geben.

- Nach Art. 39 a Abs. 3 Satz 5 BayHSchG werden den **Mitgliedern des Fachbereichs** die **wesentlichen Ergebnisse der studentischen Befragungen**, gegebenenfalls unter Hinzufügung der Stellungnahme des betroffenen Lehrenden, zugänglich gemacht. Die wesentlichen Ergebnisse sind eine personenbezogene Zusammenfassung der Bewertung durch die Studenten, die auch in der Form einer „Benotung" bestehen kann. Die „wesentlichen Ergebnisse" müssen in einer Form zugänglich gemacht werden, die eine Kenntnisnahme durch Personen, die nicht Mitglieder des Fachbereichs sind, ausschließt. Es genügt beispielsweise ein Hinweis am „Schwarzen Brett", dass Mitglieder des Fachbereichs die Möglichkeit haben, die „wesentlichen Ergebnisse" der studentischen Befragungen im Dekanat einzusehen.

Zusammenfassend ist also strikt zu trennen zwischen dem veröffentlichungsfähigen Lehrbericht und der Auswertung der Ergebnisse der studentischen Befragungen:

- Der Lehrbericht darf und muss zwar Angaben über die Bewertung des Lehrangebots durch die Studenten enthalten, nicht aber die studentischen Bewertungen im Einzelnen unter Angabe der Bezeichnung der Lehrveranstaltungen und der Namen der Lehrenden. Der Lehrbericht darf keine personenbezogenen Daten der Bewerteten enthalten; er darf daher veröffentlicht werden.

- Die Bezeichnung der Lehrveranstaltungen, die Namen der Lehrenden und die ausgewerteten Ergebnisse (d.h. also personenbezogene Daten) dürfen nur dem Fachbereichsrat und der Leitung der Hochschule bekannt gegeben und zur Bewertung der Lehre verwendet werden.

- Den Mitgliedern des Fachbereichs werden die wesentlichen Ergebnisse der studentischen Befragungen, gegebenenfalls unter Hinzufügung der Stellungnahme der betroffenen Lehrenden, zugänglich gemacht. Die wesentlichen Ergebnisse sind eine personenbezogene Zusammenfassung der Bewertung durch die Studenten, die auch in der Form einer „Benotung" bestehen kann.

In diesem Zusammenhang weise ich auch darauf hin, dass das Bayerische Staatsministerium für Wissenschaft, Forschung und Kunst zur Handhabung des Art. 39 a Abs. 3 BayHschG in der Praxis mit Schreiben vom 16.12.1999 (Gz.: X/2-23/54 947) nach Abstimmung mit mir Hinweise an die staatlichen Hochschulen gegeben hat.

Eine vollständige **Veröffentlichung der Evaluationsergebnisse** einzelner akademischer Lehrkräfte - etwa im Internet - ist meiner Auffassung nach selbst mit Einwilligung der Betroffenen datenschutzrechtlich nicht zulässig.

In Anbetracht der Überschaubarkeit und der (v.a. den Studenten) namentlich bekannten Zusammensetzung des Lehrkörpers einer Fakultät bedeutet nämlich die Veröffentlichung der „einwilligenden" Dozenten gleichzeitig inzident auch eine Veröffentlichung der Dozenten, die ihr Einverständnis zur Veröffentlichung nicht erteilt haben. Hinsichtlich dieser inzidenten Veröffentlichung liegt aber gerade keine Einwilligung vor.

Zudem besteht in dieser Situation ein faktischer Zwang für jeden Dozenten, sein Einverständnis ebenfalls zu erteilen. Diese Zwangssituation schließt aber die Annahme des Vorliegens einer datenschutzrechtlich wirksamen Einwilligungserklärung aus. Denn es ist ein wesentlicher Grundsatz des Datenschutzrechtes, dass die **Einwilligung auf der „freien Entscheidung" des Betroffenen beruhen muss.** Dieser allgemeine Rechtsgedanke ist in § 4 a Abs. 1 Satz 1 BDSG ausdrücklich niedergelegt. Eine Einwilligung kann aus datenschutzrechtlicher Sicht nur solange akzeptiert werden, wie sich die Betroffenen **nicht in einer Situation** befinden, die sie **faktisch** dazu **nötigt**, sich mit der Verarbeitung der jeweils verlangten Daten einverstanden zu erklären.

Aus diesen Gründen ist es datenschutzrechtlich nicht zulässig, die Evaluationsergebnisse (lediglich) derjenigen Dozenten zu veröffentlichen, die eine entsprechende Einwilligungserklärung zuvor abgegeben haben.

Ich bestreite nicht, dass die studentische Evaluation der Optimierung der akademischen Lehre dient und daher grundsätzlich zu begrüßen ist. Sie ist allerdings im Kern auf die Verbesserung der dienstlichen Leistungen des akademischen Lehrpersonals ausgerichtet, weshalb die für die Forschung und Lehre zur Dienstaufsicht berufenen Institutionen (der Fachbereichsrat und die Leitung der Hochschule) die bestimmungsmäßigen Adressaten der vollständigen Evaluationsergebnisse sind. Die **Evaluation** ist mithin eine **besondere Form der dienstlichen Bewertung** und muss folglich datenschutzrechtlich wie diese behandelt werden. **Öffentlich „an den Pranger" gestellt zu werden, muss kein Dozent hinnehmen.**

20.2.2 Anforderungen an Anonymisierung und Einwilligung bei Forschungsvorhaben

Durch eine Eingabe wurde ich auf ein universitäres Forschungsprojekt über den Wissensstand von Ju-

gendlichen zum Thema „Aufklärung und frühe Schwangerschaften“ aufmerksam, das in den Achten Klassen nahezu aller Schularten einer bayerischen Großstadt durchgeführt wurde.

Zu einer an einer Hauptschule durchgeführten Fragebogenaktion über „Soziales Lernen“ habe ich mich bereits in Nr. 15.2 meines 19. Tätigkeitsberichts geäußert. Dort habe ich auch (in Nr. 2.3.1) die wesentlichen Anforderungen an die datenschutzgerechte Ausgestaltung von Forschungsvorhaben dargelegt. Das im Berichtszeitraum von mir überprüfte Forschungsvorhaben gibt nunmehr Gelegenheit, die datenschutzrechtlichen Anforderungen an eine Anonymisierung personenbezogener Daten und an eine rechtswirksame Einwilligungserklärung exemplarisch darzustellen:

Anonymisierung

Die an die Schüler ausgegebenen Fragebögen enthielten zahlreiche in die persönliche Sphäre hineinreichende Fragen. In einem über die Schule verteilten „Elternbrief“ wurden die Eltern vorher kurz über den Zweck des Forschungsvorhabens unterrichtet und um Unterstützung gebeten. Im Falle von Einwänden gegen die Teilnahme des Kindes an der Befragung sollten die Eltern eine beigefügte „Widerspruchserklärung“ unterzeichnen und ihrem Kind zur Aushändigung an den jeweiligen Klassenlehrer mitgeben.

Aus datenschutzrechtlicher Sicht ist festzustellen, dass **mit den Fragebögen keine anonymen, sondern personenbezogene Daten erhoben** wurden. Die Daten waren nämlich zumindest auf bestimmte Personen beziehbar (Art. 4 Abs. 1 BayDSG). Hierfür reicht es aus, dass diese Informationen durch Merkmalskombinationen und durch Zusatzwissen auf bestimmte Personen bezogen werden können. Dabei kommt es nicht darauf an, ob im konkreten Fall die speichernde Stelle die Absicht hat, sich dieses Zusatzwissen zu besorgen. Vielmehr ist bereits die Möglichkeit der Beschaffung von Zusatzwissen ausreichend, dessen legales Bekanntwerden nach sozialüblichen Maßstäben nicht ausgeschlossen werden kann.

In den an die Schüler verteilten Fragebögen wurden zahlreiche Einzelangaben über die Jugendlichen und - mittels weiterer Fragen nach dem häuslichen Umfeld - auch über deren Eltern erhoben. Zu nennen sind hier insbesondere die Fragen nach dem Körpergewicht, der Körpergröße, dem Geburtsjahr und dem Geburtsmonat. Gerade bezüglich der beiden letztgenannten Kriterien konnte sich das zur Reidentifikation erforderliche Zusatzwissen nicht nur etwa aus internen Klassenlisten, sondern auch aus den von den Schulen veröffentlichten Jahresberichten ergeben, die neben Vor- und Zunamen auch den Geburtstag der Schüler enthalten dürfen. Die überdies verlangten Angaben zu Nationalität und Religionszugehörigkeit erhöhten die Reidentifikationsmöglichkeiten weiter. Daten, die (zumindest auch) den Eltern zuzurechnen waren, waren die Herkunft aus Deutschland, der Wohnort inner- oder außerhalb der gegenständlichen Großstadt, die Anzahl der Wohnungen in der betreffenden Gebäudlichkeit (unterteilt jeweils in vier Gruppen), die Zahl der Zimmer in der Wohnung, der Zahl der Bewohner, die Anzahl der Autos und die Anzahl der Urlaubsreisen in den letzten zwölf Monaten. Ebenfalls auch die Eltern betrafen die Fragen nach den Aktivitäten innerhalb der Familie, dem Verhältnis zu Vater und Mutter sowie nach dem Zusammenleben mit den Eltern und nach deren Berufstätigkeit.

Auf Grund dieser detaillierten Einzelangaben konnte ich - jedenfalls in Einzelfällen - nicht ausschließen, dass eine Reidentifikationsmöglichkeit zu Lasten eine(s/r) Betroffenen und damit auch seiner/ihrer Eltern bestand.

Bei der Frage, welche Anforderungen an die Identifizierbarkeit der Betroffenen zu stellen sind, habe ich auch die **Sensibilität der erhobenen Daten berücksichtigt**. Diese ist bei den Fragen in Bezug auf die Religion, das Verhältnis zu den Eltern und natürlich v.a. bei den Fragen zu Sexualität und Schwangerschaft ausgesprochen hoch. Zum großen Teil handelt es sich hier um besonders sensible Daten im Sinne von Art. 8 der EG-Datenschutzrichtlinie, Art. 15 Abs. 7 BayDSG. Meiner Meinung nach reichte deshalb auch ein noch so geringes Risiko der Identifizierung der jeweiligen Person aus, das Erheben von personenbezogenen Daten anzunehmen. Eine anonyme Befragung lag daher nicht vor.

Einwilligung

Mangels einschlägiger gesetzlicher Befugnisnorm war für das Erheben der personenbezogenen Daten eine Einwilligung der Betroffenen notwendig. Da sowohl Daten der Schüler als auch Daten der Eltern erhoben wurden, mussten sowohl eine Einwilligung der Schüler wie auch der Eltern vorliegen.

Nach den datenschutzrechtlichen Vorschriften bedurfte diese Einwilligung der Schriftform (Art. 15 Abs. 3 BayDSG); zudem musste sie sich ausdrücklich auf die sensiblen Daten beziehen (Art. 15 Abs. 7 Satz 1 Nr. 2 BayDSG). Weiter waren die Betroffenen - Jugendliche wie Eltern - auf den Zweck der Erhebung und auf die Möglichkeit hinzuweisen, die Einwilligung verweigern zu können (Art. 15 Abs. 2, Art. 16 Abs. 3 BayDSG).

Zunächst ist festzustellen, dass die den Eltern eingeräumte Möglichkeit, Widerspruch gegen die Teil-

nahme ihres Kindes an der Klassenraumbefragung zu erheben, die fehlende Einwilligung nicht ersetzen kann. Im übrigen wurden die Eltern in der „Elterninformation“ gerade nicht darüber informiert, dass mit der Umfrage auch Daten über sie selbst erhoben wurden. Folglich bezog sich auch das Widerspruchsformular gerade nicht hierauf; eine rechtswirksame Einwilligung der Eltern lag somit schon deswegen nicht vor.

Auch wurde keine datenschutzrechtlich wirksame Einwilligung der Schüler eingeholt. Bei Schülerinnen und Schülern der Achten Klassen ist grundsätzlich anzunehmen, dass sie selbst über ihr Recht auf informationelle Selbstbestimmung entscheiden können. Damit war auch ihre Einwilligung erforderlich. Von der notwendigen und nahe liegenden Möglichkeit, die gemäß Art. 15 Abs. 2, Art. 16 Abs. 3 BayDSG erforderlichen Hinweise auf die Freiwilligkeit der Datenerhebung - u.a. den ausdrücklichen Hinweis, die Einwilligung ohne nachteilige Folgen verweigern zu können - sowie auf den Zweck der Datenverarbeitung auf einem gesonderten Formblatt den Schülern zu übermitteln und sich den Empfang dieses Formblattes gesondert schriftlich bestätigen zu lassen, wurde leider kein Gebrauch gemacht. Der Hinweis auf die Freiwilligkeit der Datenangabe in der Elterninformation reichte schon deswegen nicht aus, weil er sich nicht an die Jugendlichen richtete; zudem war von der Notwendigkeit eines Einverständnisses der Jugendlichen keine Rede. Den nach Angaben der Universität lediglich mündlich gegebenen Hinweis im Klassenraum, kurz vor dem Ausfüllen der Formulare, eingerahmt von der dringenden Bitte um Teilnahme und dem In-Aussicht-Stellen einer Verlosung mit interessanten Gewinnen, habe ich schon wegen des bereits entstandenen Gruppendrucks nicht als ausreichend erachtet. Zudem erschien es mir nicht gesichert, dass der Hinweis auf die Freiwilligkeit den Jugendlichen gegenüber mit der gebotenen Deutlichkeit abgegeben wurde. Überdies fehlte auch der Nachweis, inwieweit das Erfordernis einer ausdrücklichen Einwilligung der Jugendlichen in eine Verarbeitung der sensiblen Daten im Sinne von Art. 15 Abs. 7 Satz 1 Nr. 2 BayDSG erfüllt worden war.

Datenschutzrechtlich notwendig wäre eine **Befragungsgestaltung** gewesen, die es den Schülern ermöglicht hätte, sich - sowohl von ihren Mitschülern wie von den Auswertungspersonen unbeobachtet - frei entscheiden zu können, den Fragebogen gar nicht oder nur zum Teil ausgefüllt abzugeben. Dies wäre z.B. durch die frühzeitige Ausgabe sowohl des Fragebogens als auch des Formblattes mit den Hinweisen auf Freiwilligkeit und Zweck der Datenerhebung bzw. –verarbeitung sowie des Formblattes zur Erklärung des Einverständnisses und die Abgabe des nicht/teilweise oder ganz ausgefüllten Fragebogens in einem geschlossenen Umschlag neben der gesonderten Abgabe der Erklärung über die Freiwilligkeit ohne weiteres möglich gewesen. Dieses Verfahren hätte gewährleistet, dass die **Entscheidung, an der Umfrage teilzunehmen, frei und unbeobachtet** hätte erfolgen können.

Aufgrund der zahlreichen gravierenden Verstöße gegen das Bayerische Datenschutzgesetz habe ich die Datenerhebung im Rahmen des Forschungsprojektes förmlich gem. Art. 31 Abs. 1 BayDSG beanstandet und die Anonymisierung der Daten durch Herausnahme der identifizierenden Merkmale gefordert.

20.2.3 Vorlage von Kontoauszügen bei der studentischen Rückmeldung

Einige Studenten einer Fachhochschule wandten sich an mich und berichteten über Probleme bei der Rückmeldung für das nächste Semester. Sie seien vom Studentensekretariat aufgefordert worden, als Beleg für die Entrichtung des Verwaltungskosten- und des Studentenwerksbeitrags den die Abbuchung dieser Beiträge dokumentierenden Kontoauszug vorzulegen. Andere „Beweismittel“ für die Zahlung - selbst ein mit Annahmedatum versehener und abgestempelter Überweisungsauftrag - seien als Nachweis für die Überweisung nicht akzeptiert worden. Die Studenten fürchteten, dass aus den übrigen Angaben auf dem Kontoauszug Schlüsse über ihre finanzielle Situation gezogen werden könnten (Dispositionskredit, Haben, Belastung etc.). Sie fragten bei mir an, ob sie sich gegen die Forderung des Sekretariats und die damit verbundene Einsichtnahme in ihre Geldangelegenheiten wehren könnten.

Meine Auskunft: Die Forderung nach einem Kontoauszug ist zulässig; die weiteren Daten können aber geschwärzt werden.

Im Einzelnen:

Nach Art. 65 Abs. 2 Nr. 6 BayHSchG ist ein Student u.a. zu exmatrikulieren, wenn er bei der Rückmeldung die Zahlung fälliger Gebühren oder Beiträge nicht nachweist. Damit obliegt es einerseits dem Studenten, die Zahlung der Gebühren zu beweisen; andererseits ist die Hochschule verpflichtet, bei fehlendem Nachweis den Studenten zu exmatrikulieren.

Die im Verlangen der Fachhochschule nach einem Nachweis der Beitragszahlung liegende Erhebung eines personenbezogenen Datums ist nach Art. 16 Abs. 1 BayDSG zulässig, wenn ihre Kenntnis zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben - hier also zur Durchführung des Rückmeldungsverfahrens - erforderlich ist. Da dies der Fall ist, ist das Verlangen der Fachhoch-

schule nach einem Nachweis der Beitragszahlung datenschutzrechtlich zulässig.

Dieser Nachweis kann nicht über die bloße Durchschrift des Überweisungsauftrags geführt werden. Ebensowenig kann durch die vom Kontoinhaber selbst abgestempelte Durchschrift des Überweisungsauftrags der Nachweis der Beitragszahlung erbracht werden. Denn in beiden Fällen ist es möglich, dass der Kontoinhaber den Überweisungsauftrag nicht bei der Bank abgibt. Dass die von einem Bankangestellten abgestempelte Durchschrift des Überweisungsauftrags von der Fachhochschule nicht akzeptiert wird, ist allerdings nur in der Fallgestaltung erklärlich, dass die beauftragte Bank den angenommenen Überweisungsauftrag beispielsweise wegen Überschreitung des Dispositions- und auch des geduldeten Überziehungskredits nicht ausführt. Offensichtlich hat die Fachhochschule hier schon entsprechende Erfahrungen gemacht.

In Anbetracht dieser Sachlage ist die Vorlage des die Abbuchung der Beiträge enthaltenden Kontoauszugs der sicherste Weg, die Zahlung der Beiträge nachzuweisen. Allerdings enthält der Kontoauszug über dieses personenbezogene Datum hinaus noch weitere personenbezogene Daten (Höhe des Dispositionskredits, aktueller Kontostand, andere Kontobewegungen etc.), deren Kenntnis für die Rückmeldung nicht erforderlich ist. Um die Kenntnisnahme dieser Daten durch die Fachhochschule zu verhindern, muss dem Studenten daher eingeräumt werden, die **nicht erforderlichen Daten auf dem Kontoauszug vor der Vorlage an die Fachhochschule unkenntlich zu machen** (beispielsweise zu schwärzen oder abzudecken). Hierauf ist er hinzuweisen.

21 Medien und Telekommunikation

21.1 Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Insbesondere seit der im Jahr 2002 gestarteten eGovernment-Initiative der Bayerischen Staatsregierung wird die IT-Infrastruktur in der bayerischen Verwaltung beständig ausgebaut. Damit haben immer mehr Beschäftigte die Möglichkeit, Internet und E-Mail an ihrem Arbeitsplatz zu nutzen. Dies führt allerdings nicht nur zur Erleichterung der täglichen Arbeit, sondern auch zu neuen Problemen im Verhältnis Mitarbeiter zu Dienststelle. Rechtsprechung und Literatur haben sich dieser Probleme in jüngster Zeit verstärkt angenommen. Im Hinblick auf die (arbeits-) tägliche Problematik gebe ich aus datenschutzrechtlicher Sicht folgende Hinweise:

Zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz hat bereits die 63. Datenschutzkonferenz vom 07./08.03.2002 eine Entschließung gefasst. Der Arbeitskreis Medien hat das Thema ebenfalls aufgegriffen und eine gleichnamige Orientierungshilfe verfasst. Beide Dokumente können auf meiner Homepage unter den Rubriken „Konferenzen der Datenschutzbeauftragten“ (www.datenschutz-bayern.de/dsbk-ent/63internd.pdf) und „Verwaltung - Allgemeines“ (www.datenschutz-bayern.de/verwaltung/63OHinternd.pdf) abgerufen werden. Ergänzend dazu hat der Bundesbeauftragte für den Datenschutz unter Nr. 4 der „Datenschutzrechtlichen Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz“ eine Musterdienstvereinbarung zur Verfügung gestellt (abrufbar unter www.bfd.bund.de/information/Leitfaden.pdf). Auch ich habe auf meiner Homepage Hinweise zur privaten Internet- und E-Mail-Nutzung eingestellt.

Für den Umfang der Kontrollmöglichkeiten ist es von entscheidender Bedeutung, ob der Dienstherr (bzw. Arbeitgeber) den Bediensteten lediglich die dienstliche oder auch die private Nutzung gestattet. In diesem Zusammenhang weise ich auf die für die bayerische Staatsverwaltung geltende Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) hin, die in ihrem § 10 u. a. vorgibt, dass dienstlich bereit gestellte Geräte, Programme und Netzzugänge grundsätzlich nicht für private Zwecke verwendet werden dürfen. Im Übrigen bin ich der Auffassung, dass präventive Maßnahmen gegen eine unbefugte Nutzung nachträglichen Kontrollen vorzuziehen sind.

Erlaubt die Behörde **nur die dienstliche Nutzung** von Internet und E-Mail, ist sie weder Telekommunikationsanbieter im Sinne des TKG noch Teledienesteanbieter im Sinne des TDG. Somit ist die Kontrolle der Internet- und E-Mail-Nutzung im Rahmen der Erforderlichkeit zulässig. Gegen eine Protokollierung der Zugriffe der Beschäftigten mit Tag, Uhrzeit, Beginn und Dauer der Internet-Nutzung sowie der Absender- und Zieladressen bestehen aus datenschutzrechtlicher Sicht keine Einwendungen. Der Dienstherr hat das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Dienstherrn ist als schwer wiegender Eingriff in das Persönlichkeitsrecht des Beschäftigten dagegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Bei ausschließlich erlaubter dienstlicher Nutzung darf der Dienstherr auch von ein- und ausgehenden E-Mails seiner Beschäftigten im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Datenschutzrechtlich zulässig ist also beispielsweise eine Verfügung des Vorgesetzten, ihm jede ein- oder

ausgehende dienstliche E-Mail seiner Mitarbeiterinnen und Mitarbeiter zur Kenntnis zu geben. (Vgl. zum Ganzen Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, Teil C, Handbuch XIV.10.c aa und d aa.)

Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem **besonderen Vertrauensverhältnis** zu den betroffenen Personen stehen (z.B. Psychologen, Ärzte, Sozialarbeiter und -pädagogen), muss nach der Rechtsprechung des Bundesarbeitsgerichts zu Verbindungsdaten über dienstliche Telefonate eine Kenntnisnahme des Dienstherrn vom Inhalt der Nachrichten und den Verbindungsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden. Die Nutzungs- und Verbindungsdaten der **Personalvertretung** dürfen nur insoweit kontrolliert werden, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Fallen aber - was überwiegend der Fall sein wird - nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail an, ist eine Auswertung dieser Daten unzulässig.

Gestattet der Dienstherr **auch die private Nutzung** von Internet und E-Mail, so muss er sich vielfältigen Rechtsproblemen stellen. Der Dienstherr ist hier Telekommunikationsanbieter im Sinne des TKG und Teleddiensteanbieter im Sinne des TDG. Damit gilt das Fernmeldegeheimnis gem. § 88 TKG. Das Fernmeldegeheimnis umfasst nicht nur den Inhalt der Kommunikation, sondern auch deren nähere Umstände (Wer hat mit wem kommuniziert ?). Nach § 88 Abs. 3 TKG ist es untersagt, sich über das für die Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Im Falle der Zulassung der privaten Nutzung ist daher, wenn sich - wie in der Regel - die private von der dienstlichen Nutzung technisch nicht trennen lässt, die Protokollierung nur zulässig, soweit sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs oder für Abrechnungszwecke erforderlich ist oder die Betroffenen eingewilligt haben. Aus diesem Grund kann der Dienstherr die Gestattung der privaten Nutzung davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen. Wird eine Protokollierung aufgrund der (informierten) schriftlichen Einwilligung des Beschäftigten vorgenommen, ist allerdings eine Auswertung von Protokollen nur im Rahmen dieser Einwilligung zulässig. Ich weise darauf hin, dass diese ausdrückliche Einwilligung nicht durch eine Regelung in einer Dienstvereinbarung ersetzt werden kann. (Vgl. zum Ganzen Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar, Teil C, Handbuch XIV.10.c bb und d bb.)

Nach Art. 75 a Abs. 1 Nr. 1 BayPVG hat der **Personalrat** sowohl im Fall der rein dienstlichen als auch im Fall der zugelassenen privaten Nutzung über Kontrollmaßnahmen (insbesondere Protokollierung und Auswertung) zur Internet- und E-Mail-Nutzung am Arbeitsplatz **mitzubestimmen**, da es sich in jedem Fall um eine Verhaltenskontrolle handelt. Aus datenschutzrechtlicher Sicht empfehle ich, über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden (vgl. Art. 73 Abs. 1 Satz 1 BayPVG).

Schließlich sollten die **Beschäftigten umfassend darüber informiert werden**, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert. Insbesondere sind sie auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen hinzuweisen.

21.2 Verhinderung einer datenschutzwidrigen Neuordnung der Rundfunkfinanzierung

Die Datenschutzbeauftragten des Bundes und der Länder setzen sich bereits seit langem für Datenvermeidung und Datensparsamkeit auch bei der Finanzierung des öffentlich-rechtlichen Rundfunks ein (vgl. nur die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13.10.2000; Datensparsamkeit bei der Rundfunkfinanzierung).

Im Jahr 2003 bereiteten die Länder eine grundlegende Neuordnung der Rundfunkfinanzierung vor. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten ließen zum Teil **gravierende Verschlechterungen des Datenschutzes befürchten:**

- So sollten die Meldebehörden verpflichtet werden, der GEZ die Daten aller über 16-jährigen Personen zu übermitteln. Dadurch wäre bei der GEZ faktisch ein bundesweites, zentrales Register mit Informationen über die sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen) entstanden, obwohl ein großer Teil dieser Daten für den Einzug der Rundfunkgebühren überhaupt nicht erforderlich gewesen wäre.

- Nach den ursprünglichen Plänen der Länder sollten zwar in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden. Dennoch sollten alle dort gemeldeten

erwachsenen Bewohner - auch ohne Anhaltspunkte für eine Gebührenpflicht - zur Auskunft verpflichtet sein. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst - wie bei den amtlichen Statistiken erfolgreich praktiziert - nur die Meldedaten derjenigen Person übermittelt werden, die dazu auch befragt wird.

- Zudem war beabsichtigt, die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten um Übermittlungen aus weiteren staatlichen oder sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister zu erweitern; auf alle diese Dateien war ein Online-Zugriff der GEZ geplant.

- Gleichzeitig sollte die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten - wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern - zu erheben, ausdrücklich erlaubt werden.

In Reaktion auf diese Vorschläge hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf der Basis eines auch unter meiner Mitwirkung erstellten Entwurfes des Arbeitskreises Medien und Telekommunikation am 30.04.2003 die Entschließung „Neuordnung der Rundfunkfinanzierung“ (vgl. Anlage 9) gefasst, mit der die zentralen datenschutzrechtlichen Kritikpunkte öffentlich gemacht wurden.

Nicht zuletzt auf Grund dieser Entschließung haben die Länder in der Folgezeit „schwer widerlegbare datenschutzrechtliche Bedenken“ gegen die Reformvorschläge angebracht und von der Umsetzung der geplanten Neuordnung der Rundfunkfinanzierung Abstand genommen.

22 Technischer und organisatorischer Bereich

22.1 Grundsatzthemen

22.1.1 Bayerisches Behördennetz (BYBN, BayKOM)

22.1.1.1 Sicherheitsorganisation und –richtlinien

Im Berichtszeitraum lief der Rahmenvertrag mit bol Behörden Online GmbH über den Betrieb des Bayerischen Behördennetzes aus. Nach einer Ausschreibung, in der auch wesentliche Anpassungen im organisatorischen sowie im sicherheitstechnischen Bereich beim Behördennetz vorgenommen wurden, wurde die Firma BT Ignite GmbH & Co. OHG, München, mit der Fortführung des Bayerischen Behördennetzes (BYBN) und der Bereitstellung des zentralen Internetzugangs beauftragt (siehe Kapitel 17.1.1 des 20. Tätigkeitsberichts).

Mit Bekanntmachung vom 15.6.2004 hat die Bayerisches Staatsregierung die „Richtlinie für den koordinierten Einsatz der Informations- und Kommunikationstechnik (IuK) in der bayerischen Staatsverwaltung (IuK-KoordR)“ erlassen. Diese regelt die künftige IuK-Strategie innerhalb der bayerischen Staatsverwaltung. Dazu zählen unter anderem das Bayerische Behördennetz und auch Verfahren für Verschlüsselung und Signatur.

Zur Umsetzung dieser Strategie wurde im Staatsministerium des Innern die Zentrale IuK-Leitstelle (ZIL) eingerichtet. Der geschäftsbereichübergreifende, beim Staatsministerium der Finanzen eingerichtete IuK-Fachausschuss steht der ZIL als beratendes Gremium zur Seite. Aufgabe der ZIL ist es, die notwendigen Richtlinien und Standards sowie die zu ergreifenden technisch-organisatorischen Maßnahmen zur Datensicherheit und zum Datenschutz verbindlich festzulegen und für deren Einhaltung und Überwachung zu sorgen. So hat die ZIL die „IT-Sicherheitsleitlinie für die bayerische Staatsverwaltung (IT-Security Policy)“ erarbeitet. Darin wird ein gemeinsames Sicherheitsniveau definiert und eine entsprechende Sicherheitsorganisation etabliert.

Als zentrale Instanz dieser Sicherheitsorganisation fungiert der Chief Information Security Officer (CISO), der sich eines beratenden Sicherheitsteams bedient. Das Sicherheitsteam wiederum setzt sich aus den Beauftragten für IT-Sicherheit der Staatskanzlei, der Staatsministerien, des Obersten Rechnungshofs, des Landtagsamts und meiner Dienststelle sowie einem Computer Emergency Response Team (CERT) zusammen. Bisher wurden von diesen Gremien be-

reits umfangreiche Sicherheitsrichtlinien (BayITSRL) erarbeitet und der ZIL zur Verabschiedung zugeleitet.

Durch diese Maßnahmen dürfte eine Grundlage für meine schon lange angemahnte Schaffung einer kompetenten und geschäftsbereichübergreifend bindenden Instanz für die Sicherheit der elektronische Kommunikation innerhalb des Bayerischen Behördennetzes geschaffen sein. Diese gilt es in nächster Zeit noch weiter auszufüllen.

22.1.1.2 Elektronische Signatur und Verschlüsselung

Für die sichere elektronische Kommunikation per E-Mail mit den Bürgern bieten inzwischen viele, wenn auch nicht alle staatlichen Behörden auf ihren Webseiten PGP Schlüssel an. Damit können Personen außerhalb des Behördennetzes sicher und vertraulich mit den jeweiligen Poststellen der Behörden E-Mails austauschen.

Wie schon in meinem letzten Tätigkeitsbericht erwähnt, konnte auch in diesem Berichtszeitraum nicht erreicht werden, dass ein nennenswerter Anteil von E-Mails zwischen den Behörden unter der Verwendung von S/MIME digital signiert oder verschlüsselt wird. Es wurden zwar einige tausend Zertifikate vom Statistischen Landesamt für Datenverarbeitung ausgegeben, sodass sich die Voraussetzungen für den Einsatz verbessert haben. Damit ist eine ausreichende Flächendeckung aber immer noch nicht erreicht, was auch an der nach wie vor zu heterogenen Softwarelandschaft liegt. Des Weiteren fehlt es aber anscheinend auch gelegentlich an der Motivation der einzelnen Behörden, E-Mails zu verschlüsseln und zu signieren.

22.1.1.3 Zentralisierung von Rechnerleistung

In Abschnitt 17.1.2 meines 19. Tätigkeitsberichts 2000 vom 14.12.2000 hatte ich ausgeführt, dass ich die heterogene technische und personelle Ausstattung der Teilnehmer am Bayerischen Behördennetz, d.h. die Heterogenität der IuK-Binnenstruktur in der bayerischen Staatsverwaltung, als mit ursächlich für die bestehenden Sicherheitsprobleme halte.

Einige wesentliche Merkmale dieser Struktur sind

- das Bestehen staatlicher Rechenzentren, z.B. beim Landesamt für Statistik und Datenverarbeitung, beim Technischen Finanzamt Nürnberg, beim Landeskriminalamt sowie in einigen Ministerien für deren nachgeordnete Bereiche, die sowohl eigene Aufgaben erledigen als auch z.T. als Dienstleistungsrechenzentren genutzt werden

- die unterschiedlich starke IT-Durchdringung der staatlichen Verwaltung,

- das z.T. bis auf Dienststellenebene eigenverantwortliche Auswählen, Beschaffen, Betreiben und Fortentwickeln von IuK-Einrichtungen und Software,

- daraus resultierend unterschiedlichste IuK-Ausstattungen bzgl. Hard- und Software in den IT-Betriebsstellen sowie

- z.T. Mangel an qualifiziertem EDV-Fachpersonal in den jeweiligen IT-Betriebsstellen.

In Anbetracht der Tatsache, dass die Bedeutung der IuK-Technologien für die öffentliche Verwaltung in der Vergangenheit sehr rasch zugenommen hatte und der IuK-Einsatz für die meisten Verwaltungsdienstleistungen zum maßgeblichen Faktor bezüglich Effizienz und Bürgerfreundlichkeit geworden waren, wurde im November 2001 der damalige Koordinierungsausschuss Datenverarbeitung (KoA DV) beauftragt, zu den Rechenzentren der staatlichen Verwaltung und den darauf laufenden Anwendungen eine Bestandsaufnahme durchzuführen sowie erste Überlegungen zu effizienzsteigernden Strukturen und zum Outsourcing von Leistungen der Rechenzentren vorzunehmen. Ziele dieser Bestandsaufnahme waren wie folgt:

- Gewährleistung der Sicherheit in der IuK-Technik und Daten: Zugangsschutz, Backup (räumliche Trennung), Ausfallrechenzentren

- Sicherstellung der Verfügbarkeit von Informationen und Diensten: 24 Std-Betrieb/365 Tage (Hochverfügbarkeit)

- Steigerung der Leistungsfähigkeit und Wirtschaftlichkeit durch Bündelung von IuK-Dienstleistungen

- Konsolidierung der Betriebssysteme unter Beachtung möglichster Herstellerunabhängigkeit

- Sicherung der Akzeptanz der benötigten IuK-Dienstleistung

Anlässlich einer Sondersitzung des damaligen Koordinierungsausschusses IuK (KoA IuK, Nachfolger des KoA DV) am 10.01.2003 wurde von der Staatskanzlei das mit Hilfe eines externen Unternehmens

beabsichtigte Projekt „Untersuchung zur Konsolidierung von Rechen- und IT-Betriebszentren der Staatsverwaltung“ vorgestellt. Ziel dieser Untersuchung sollte sein, die Zahl der Rechen- und IT-Betriebszentren vorwiegend aus Wirtschaftlichkeitsgründen drastisch zu reduzieren und die IuK-Ausstattung weitestmöglich zu vereinheitlichen.

Unmittelbar im Nachgang zu dieser Sondersitzung habe ich vorsorglich die Staatskanzlei und die Mitglieder des KoA IuK schriftlich auf folgende Aspekte hingewiesen:

- Die in der Leistungsbeschreibung zum Projektvertrag erhobene Forderung, dass das Soll-Konzept auch den Aspekten des Datenschutzes und der Sicherheit Rechnung tragen müsse, würde ausdrücklich begrüßt.

- Das Vorhaben berge aber u.U. erhebliches Gefahrenpotenzial für die Sicherstellung des Datenschutzes im staatlichen Bereich - nicht zuletzt dadurch, dass zentrale Datenbestände erfahrungsgemäß generell Begehrlichkeiten wecken.

- Vor dem letztendlichen Ziel der Untersuchung, die Anzahl der derzeit vorhandenen Rechen- und IT-Betriebszentren zu reduzieren, könnten die Datenschutz- und Datensicherheitsaspekte sowohl aus rechtlicher als auch aus technisch-organisatorischer Sicht einen ausgesprochen komplexen Umfang annehmen - je nach Umfang der vorgeschlagenen Konsolidierungsmaßnahme und den davon betroffenen zu verarbeitenden personenbezogenen Daten.

- Meinerseits bestünden erhebliche Zweifel, dass diese Thematik in der für die Untersuchung zur Verfügung stehenden knappen Zeit ausreichend beleuchtet und berücksichtigt werden könne. Dabei sei insbesondere zu berücksichtigen, dass bereichsspezifische Vorschriften dem Bayerischen Datenschutzgesetz vorgehen und zum Teil eine Auftragsdatenverarbeitung/ein Outsourcing aus Geheimhaltungspflichten verböten. Es erscheine fraglich, dass alle Dienststellen, die den Fragebogen zum Ausfüllen vorgelegt erhalten, diese Problematik an dieser Stelle und zu diesem Zeitpunkt erkennen und die hier erforderlichen Angaben im Fragebogen vollständig machten.

- Wegen der oben dargestellten Komplexität der vorab zu klärenden rechtlichen und technisch-organisatorischen Fragestellungen könne u.U. auch sehr schnell der Zustand erreicht werden, dass die Erreichung der mit der Konsolidierung angestrebten Ziele aufgrund zu ergreifender Sicherheitsmaßnahmen infrage gestellt oder gar verfehlt würden.

Am 29.07.2003 hat der Ministerrat entschieden, dass die bisherigen Rechen- und IT-Betriebszentren der Staatsverwaltung organisatorisch in zwei Rechenzentren (Nord und Süd) zusammengefasst werden. Die Staatskanzlei und die Ministerien können unter Berücksichtigung von Sicherheit und Wirtschaftlichkeit des Betriebs ihre IuK-Anwendungen aber auch von privaten Rechenzentren betreiben lassen. In einem ersten Schritt sollen 150 IT-Betriebszentren sukzessive organisatorisch in eines der beiden Rechenzentren eingegliedert und anschließend die entsprechenden IuK-Einrichtungen nach technischen und wirtschaftlichen Gesichtspunkten physikalisch konsolidiert werden.

An dieser Stelle wiederhole ich meine bei verschiedensten Gelegenheiten geäußerten Bedenken gegen zentrale Datenbestände, weil diese generell Begehrlichkeiten entwickeln, die mit der zunehmenden Automatisierung und Vernetzung der Datenverarbeitung noch wachsen.

Ich weise überdies deutlich darauf hin, dass

- der Grundsatz der informationellen Gewaltenteilung jedenfalls in jedem Einzelfall weiterhin sicherzustellen ist,

- Verstöße gegen Datenschutz und Datensicherheit bei zentralen Datenbeständen und IuK-Einrichtungen ungleich schwerer wiegen als bei dezentralen Datenbeständen mit weniger Daten,

- es sich bei der Übertragung der Datenverarbeitung an die beiden Rechenzentren um Auftragsdatenverarbeitung i.S.d. Art. 6 BayDSG handeln kann und dessen Bestimmungen dann unbedingt zu beachten und einzuhalten sind, ggf. ist sogar aufgrund spezialgesetzlicher Bestimmungen eine Auftragsdatenverarbeitung nicht zulässig,

- die Datentrennung, die Geheimhaltung, die Zugriffsbeschränkungen und die Zweckbindungen für die erhobenen Daten durch diese Zentralisierungen nicht tangiert oder gar unterlaufen werden dürfen und

- dem Stand der Technik entsprechende und geeignete Maßnahmen ergriffen werden müssen, um die Authentizität, Integrität und Vertraulichkeit der zwischen den Rechenzentren

bzw. IuK-Betriebsstellen und den jeweiligen Behörden übertragenen schutzwürdigen Daten sicherzustellen.

22.1.2 Viren- und Spam-Filterung

Immer mehr Dienststellen beabsichtigen, ein sicheres und leistungsfähiges Intranet für ihre Verwaltungen und andere angeschlossenen öffentlichen Stellen (z.B. Kommunen eines Landkreises) zu errichten. Viele dieser Behördennetze bestehen bereits und sind auch an das Bayerische Behördennetz angeschlossen. Zur Gewährleistung der Datensicherheit innerhalb des eigenen Intranets sollte vom Betreiber dieses Netzes ein entsprechendes Sicherheitskonzept erarbeitet werden, in dem auch die Handhabung virenverdächtiger E-Mails bzw. Spam-Mails geregelt sind.

Bei der Durchsicht derartiger uns vorliegender Sicherheitskonzepte ist uns aufgefallen, dass Unklarheit darüber besteht, ob virenverdächtige E-Mails bzw. Spam-Mails beim Netzbetreiber gelöscht bzw. unterdrückt (geblockt) werden sollen oder ob sie an die Adressaten bei den angeschlossenen Stellen weiterzuleiten sind. Ich darf daher in diesem Zusammenhang auf Folgendes hinweisen:

1. Löschung bzw. Blockung von E-Mails, die gefährlichen oder verdächtigen ausführbaren Code enthalten, bei Gestattung der ausschließlich dienstlichen Nutzung

Es ist richtig, dass aus Gründen der Datensicherheit (dienstliche) E-Mails oder Anlagen von E-Mails gelöscht bzw. unterdrückt (geblockt) werden sollten, die gefährlichen oder verdächtigen ausführbaren Code enthalten (z.B. E-Mails mit HTML-Seiten als Mail-body oder Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha).

Solange diese Löschung oder Blockung von E-Mails auf Rechnern der adressierten bzw. absendenden Behörde erfolgt und eine private E-Mail-Nutzung verboten ist, bestehen auch von Seiten des Datenschutzes keinerlei Bedenken gegen diese Vorgehensweise. Anders sieht es allerdings aus, wenn statt einer Löschung eine Blockung bei einer anderen Stelle (z.B. beim Landratsamt als Netzbetreiber eines Kommunalen Behördennetzes) erfolgt. Denn auch geblockte E-Mails können personenbezogene Daten beinhalten, womit bei einer Blockung dieser E-Mails und einem Abspeichern auf einem Rechner beim Netzbetreiber ein (unberechtigter) Zugriff auf diese Daten seitens seiner Bediensteten möglich wäre.

Somit muss – bei einer rein dienstlichen Nutzung des E-Mail-Verkehrs (Verbot der Privatnutzung bei **allen** angeschlossenen Stellen) – zumindest vertraglich ein unberechtigtes Öffnen der geblockten E-Mails verboten werden bzw. eine unverzügliche Löschung der betreffenden E-Mails vereinbart werden. Außerdem sollte bei einer ausgehenden E-Mail der Absender von dem Vorgehen informiert werden.

2. Löschung oder Blockung von E-Mails, die gefährlichen oder verdächtigen ausführbaren Code enthalten, bei Gestattung der privaten Nutzung

Gestattet dagegen eine Dienststelle als Arbeitgeber ihren Bediensteten die private Nutzung des Internets und des E-Mail-Dienstes, ist sie ihnen gegenüber Telekommunikations- bzw. Teledienste-Anbieter und zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG verpflichtet (vgl. Nr. 21.1).

Einerseits ist private E-Mail grundsätzlich ohne vorherige Kenntnisnahme des Inhalts an den Adressaten weiterzuleiten, andererseits dürfen - wie bei der dienstlichen Nutzung - aus Gründen der Datensicherheit auch eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das ausführbaren Code enthalten kann. Eine weitere Möglichkeit besteht darin, erkannte Viren automatisch aus den E-Mails zu entfernen und die gesäuberte E-Mail weiterzuleiten.

Die gewählte Verfahrensweise ist mit dem Personalrat abzustimmen und den Beschäftigten zuvor bekannt zu geben. Die Mitarbeiter sollten zu dieser Vorgehensweise eine schriftliche Einwilligung erteilen.

Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind.

3. Blocken von Spam-Mails

Das Versenden bzw. Empfangen von unerwünschter Post mittels E-Mail (so genannte Spam-Mails) ist an sich kein Datenschutzproblem. Allerdings stellt es ein Ärgernis dar und belastet die Ressourcen in erheblichem Masse. Solche Sendungen können insbesondere zu Behinderungen der Arbeit führen; im Extremfall ist eventuell überhaupt keine Kommunikation mehr möglich. Zudem können auch erhöhte Kommunikationsgebühren entstehen. Somit besteht natürlich ein dienstliches Interesse daran, auch diese E-Mails zu filtern und zu blocken.

Eine weitere Möglichkeit würde darin bestehen, die Annahme von vermeintlicher Spam-Mail automatisch zu verweigern und an den Absender zurückzusenden. Dies birgt aber die Gefahr, dass der Absender er-

kennt, dass die gespamte E-Mail-Adresse existiert und er nur sein Spam-Verhalten zur Vermeidung einer erneuten Filterung verbessern muss.

Außerdem muss damit gerechnet werden, dass aufgrund der derzeitigen Schwächen der eingesetzten Filterungssoftware eventuell auch „sinnhafte“ E-Mails als Spam-Mails behandelt und somit nicht weitergeleitet werden würden (False-Positive-Filterung). Dies kann auch zu Haftungsproblemen führen.

So lange eine hundertprozentig zuverlässige Spam-Filterung von E-Mails technisch nicht möglich ist, sollten auch augenscheinliche Spam-Mails nur entsprechend gekennzeichnet werden. Bei gestatteter privater E-Mail-Nutzung dürfen diese nicht geblockt, sondern müssen an den Empfänger weitergeleitet werden. Diese Vorgehensweise wird auch im Bayerischen Behördennetz praktiziert.

Der Empfänger kann dann selbst sein weiteres Vorgehen bestimmen. So besteht bei den meisten E-Mail-Clients die Möglichkeit, beispielsweise E-Mails, welche von Absendern stammen, die dem Empfänger als Spammer bekannt sind (Black List), mittels Regel auszusortieren. Eine weitere Möglichkeit besteht darin, vermeintliche Spam-Mails in einem gesonderten Ordner bis zu einem vorher bestimmten Verfallsdatum, bis zu einer bestimmte Menge oder bis zur manuellen Löschung durch den Empfänger abzulegen.

Zusammenfassend möchte ich noch einmal darauf hinweisen, dass jegliche Art von Filterung beim Netzbetreiber vertraglich zu verankern ist. Zusätzlich ist bei einer gestatteten privaten E-Mail-Nutzung die Einwilligung jedes einzelnen Betroffenen zur gewählten Vorgehensweise erforderlich.

22.1.3 Verzeichnisdienste

Da immer mehr Behörden auf elektronischem Weg miteinander kommunizieren und sich zum Teil zusammen mit anderen Behörden zu eigenen Netzen (kommunale Behördennetze, Bayerisches Behördennetz etc.) zusammenschließen, stellt sich die Frage nach einem behördenübergreifenden Verzeichnisdienst immer mehr. Die klassische Trennung der Netzwelt in zwei Bereiche, Intranet als behördeninternes und Internet als weltweites Netz, trifft hier nicht mehr zu.

Wie sieht es dann aber mit dem Datenschutz aus? Darf man Daten, die man im eigenen Verzeichnisdienst im Intranet veröffentlichen darf, auch im Behördenverzeichnisdienst veröffentlichen, oder dürfen dort nur Daten publiziert werden, die auch für das Internet zulässig wären?

Für nicht personenbezogene Daten, wie Funktionsadressen und Dienststellendaten, bestehen weder für das Internet noch für das Behördenintranet datenschutzrechtliche Einschränkungen; diese dürfen auch in behördenübergreifende Verzeichnisdienste aufgenommen werden.

Für personenbezogene Daten ist darauf zu achten, dass die Sichtbarkeit der Daten außerhalb der eigenen Behörde eingeschränkt werden kann. Grundsätzlich sollen auch in einem Verzeichnisdienst nur die personenbezogenen Daten in dem jeweiligen Anwenderkreis sichtbar sein, die zur ordnungsgemäßen Aufgabenerfüllung dieses Kreises notwendig sind. Der Grundsatz der Erforderlichkeit gilt auch für die Veröffentlichung einzelner Daten bestimmter Mitarbeiter. Im Übrigen verweise ich auf die Ausführungen in Kapitel 12.3 meines 18. Tätigkeitsberichts und Kapitel 13.1.4 meines 20. Tätigkeitsberichts. Somit sollte zum einen ein Datenfeld nur im kleinsten benötigten Anwenderkreis standardmäßig sichtbar sein, zum anderen muss es auch möglich sein, auf Wunsch eines Mitarbeiters normalerweise sichtbare Daten nicht zu veröffentlichen, wenn der Mitarbeiter daran ein berechtigtes Interesse hat.

Damit ergibt sich für die Sichtbarkeit von Informationen ein Schalenmodell, das von innen nach außen einem immer größeren Anwenderkreis Zugriff auf die Daten erlaubt. Für einen bayernweiten Verzeichnisdienst wäre dies beispielsweise:

- Schale 1: staatliche Behörde (Intranet)
- Schale 2: staatliche Verwaltung / unabhängige staatliche Behörden
- Schale 3: bayerische Verwaltung
- Schale 4: Internet

Für jeden Datentyp im Verzeichnisdienst muss festgelegt werden, wie weit die darin beinhalteten Daten die eigene Schale (Intranet) verlassen dürfen.

22.1.4 Gütesiegel für datenschutzfreundliche Produkte

Im Berichtszeitraum haben sich mehrfach Unternehmen mit der Frage an mich gewandt, ob ich ihre Produkte (Software, Hardware) aus Datenschutzgesichtspunkten bewerten und ggf. zertifizieren kann, weil sie diese Produkte im Bereich der öffentlichen Verwaltung zum Einsatz bringen wollen oder bereits zum Einsatz gebracht haben. Eine Produktzertifizierung gehört derzeit nicht zu meinen Aufgaben.

In § 9a Bundesdatenschutzgesetz ist ein Datenschutzaudit normiert. Bislang ist mir aber noch kein Gesetzentwurf bekannt, in dem dieses Datenschutzaudit näher präzisiert wird. So kann von allen meinen Kollegen auf Landes- und Bundesebene derzeit lediglich mein Kollege vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) anhand der dortigen Datenschutzauditverordnung Schleswig-Holstein einen solchen Service bieten und ein Datenschutz-Gütesiegel vergeben. Durch das i.d.R. auf zwei Jahre befristete Gütesiegel wird bescheinigt, dass ein Produkt einem förmlichen Prüfungsverfahren hinsichtlich seiner Konformität zu den Vorschriften über den Datenschutz und die Datensicherheit unterzogen wurde und diese gegeben ist. Das Gütesiegel wird vom ULD auf Basis eines Gutachtens verliehen, welches von den beim ULD akkredierten Sachverständigen und sachverständigen Prüfstellen erstellt wird. Ergänzend sollen nach dem Landesdatenschutzgesetz Schleswig-Holstein vorrangig solche Produkte eingesetzt werden, die mit dem Datenschutz-Gütesiegel ausgezeichnet wurden.

Es sollte geprüft werden, ob eine Regelung über die Zertifizierung von Produkten auch in Bayern eingeführt werden sollte. Dies hätte aus meiner Sicht folgende Vorteile:

- Hersteller: Gezielteres Bewerben eines zertifizierten Produktes möglich und gesteigerte Produktqualität erreichbar

- Öffentliche Verwaltung: leichtere Auswahl geeigneter Produkte, die mit den Vorschriften des Datenschutzes in Einklang stehen, d.h. zeit- und kostenaufwändige Prüfungen der Produkte und Verhandlungen mit dem Hersteller bzgl. Anpassungen und Änderungen aufgrund von Datenschutzforderungen entfallen

- Meine Dienststelle: Effizientere, da erleichterte Kontrolle der Einhaltung der Datenschutzvorschriften bei Verwendung zertifizierter Produkte in der öffentlichen Verwaltung

- Der Bürger: Zuverlässige Gewissheit, dass seine Daten in der öffentlichen Verwaltung mit Produkten verarbeitet werden, die von unabhängigen und sachverständigen Gutachtern auf die Einhaltung von Datenschutz und Datensicherheit geprüft wurden, wobei Schwerpunkte auf Datenvermeidung und Datensparsamkeit, Datensicherheit und Revisionsfähigkeit gelegt werden.

Das Staatsministerium des Innern ist der Auffassung, dass wegen der vorhandenen Datenschutzkontrollinstanzen ein zusätzliches Audit nicht notwendig sei. Durch ein Audit würde neben der Selbstkontrolle durch behördliche und betriebliche Datenschutzbeauftragte und der Fremdkontrolle durch die Datenschutzkontrollbehörden nunmehr eine dreifache Kontrolle eingeführt werden. Dies sei auch angesichts der Kosten nicht vertretbar.

Diese Fragen könnten im Rahmen einer Prüfung im einzelnen beantwortet werden.

22.1.5 Pseudonymisierte Protokolle

In Kapitel 17.3.1 meines 20. Tätigkeitsberichts bin ich auf die Protokollauswertung auf Firewallsystemen und Webservern eingegangen. Das Problem, Protokolldateien mit den Anforderungen des Datenschutzes in Einklang bringen, stellt sich aber nicht nur dort – es trifft prinzipiell auf jede Protokollierung zu, die mit und von IuK-Systemen erstellt wird.

Art. 7 Abs. 2 Ziffern 6 und 7 BayDSG fordern implizit eine Protokollierung, um

- überprüfen und feststellen zu können, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können und

- nachträglich überprüfen und feststellen zu können, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.

Art. 7 Abs. 2 Ziffer 10 BayDSG fordert überdies, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Zu diesen Anforderungen gehören auch die Sicherstellung der Verfügbarkeit der Systeme sowie die Möglichkeit, eventuelle Angriffe und Sicherheitsverletzungen erkennen und diesen nachgehen zu können. Auch daraus ergibt sich der Zwang, Protokolldateien anzulegen.

Nun besteht aber das Dilemma, dass einerseits Protokolldaten anzulegen sind, andererseits aber damit personenbezogene Daten gespeichert werden, ohne dass evtl. zunächst erkennbar sicherheitsrelevante Ereignisse vorliegen – weil deren Erkennung ggf. längere Zeit in Anspruch nimmt. Derjenige, dessen Aktivitäten protokolliert werden, hat natürlich ein Interesse und grundsätzlich auch einen Rechtsanspruch darauf, diese seine Aktivitäten anonym durchführen zu können. Der Betreiber eines IuK-Systems hat aber natürlich ein Interesse, evtl. Sicherheitsver-

letzungen entdecken und diesen dann konkret nachgehen zu können.

Einen aus Datenschutzsicht sehr interessanten und zielführenden Ansatz zur Lösung dieses Dilemmas verfolgt das Konzept Pseudo/CoRe, welches im Rahmen eines Forschungsauftrags an der Universität Dortmund entwickelt wurde. Es ist auf verschiedenen UNIX-Systemen getestet worden und wurde auch anlässlich der CeBIT 2003 der Öffentlichkeit vorgestellt. Pseudo/CoRe basiert darauf, dass bereits bei der Erstellung von Protokolldatensätzen die vorab festzulegenden und zu verfremdenden Bestandteile der Potokolldatensätze durch Pseudonyme unterschiedlichster Art ersetzt werden. Außerdem werden gemeinsam mit dem örtlichen Datenschutzbeauftragten ebenfalls im Vorfeld bestimmte Merkmale (Schwellwerte) definiert, die einen Anfangsverdacht für eine Sicherheitsverletzung darstellen und automatisch aufdeckbar werden sollen. Stellt sich erst im Nachhinein heraus, dass bestimmte weitere Anhaltspunkte für eine Sicherheitsverletzung vorhanden sind, so können diese pseudonymisierten Daten auch nur wieder in Zusammenarbeit mit dem örtlichen Datenschutzbeauftragten aufgedeckt werden. Durch die technische Zweckbindung bei der Pseudonym-Aufdeckung werden bereits bei der Protokollerstellung die Interessen nach Anonymität einerseits und Zurechenbarkeit andererseits in einen fairen Ausgleich gebracht.

Ich habe das Bayerische Landesamt für Statistik und Datenverarbeitung, als Betreiber des zentralen Internetübergangs aus dem Bayerischen Behördennetz, auf Pseudo/CoRe aufmerksam gemacht.

22.1.6 Bestellung eines gemeinsamen Datenschutzbeauftragten für mehrere Städte

Ich hatte mich mit der Absicht dreier Städte zu befassen, für alle drei Städte einen gemeinsamen Datenschutzbeauftragten zu bestellen.

Gemäß Art. 25 Abs. 2 BayDSG haben alle öffentliche Stellen in Bayern, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen. Diese Vorschrift zur Bestellung eines behördlichen Datenschutzbeauftragten beruht auf Art. 18 Abs. 2 Spiegelstrich 2 EG-Datenschutzrichtlinie. Nach dieser Regelung entfallen die zwingend vorgeschriebenen Meldepflichten der Behörden gegenüber der Datenschutzkontrollstelle - für bayerische Behörden also gegenüber dem Landesbeauftragten für den Datenschutz - und die Vorabkontrollen durch die Datenschutzkontrollstelle nur dann, wenn von diesen Behörden behördliche Datenschutzbeauftragte ernannt werden. Diesen obliegt insbesondere die unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen (also dem BayDSG).

Die EG-Datenschutzrichtlinie geht davon aus, dass eine Ausnahme von der Meldepflicht nur dann zulässig ist, wenn vor Ort durch den behördlichen Datenschutzbeauftragten sichergestellt wird, dass „die Rechte und Freiheiten der Betroffenen durch die Verarbeitung nicht beeinträchtigt werden". Dies verlangt, dass eine effektive Kontrolle vor Ort möglich sein muss. Eine derartig effektive Kontrolle setzt voraus, dass diese Stelle personalmäßig so ausgestattet ist, dass sie ihren Aufgaben gerecht werden kann. Dabei sind die Anforderungen umso höher, je größer die zu kontrollierenden Stellen sind.

Diese Verpflichtung ist bei der Entscheidung zu Grunde zu legen, ob von der Regelung in Art. 25 Abs. 2 Satz 2 BayDSG, wonach aus Gründen der Verwaltungsvereinfachung mehrere öffentliche Stellen einen gemeinsamen Datenschutzbeauftragten bestellen können, Gebrauch gemacht werden kann.

In der Gesetzesbegründung zu Art. 25 Abs. 2 BayDSG (LT-Drs. 14/3327 vom 04. 04. 2000) wird als Beispiel genannt, dass mehrere Gemeinden miteinander oder auch ein Landratsamt mit Gemeinden einen gemeinsamen behördlichen Datenschutzbeauftragten bestellen. Der Gesetzgeber wollte mit dieser Vorschrift der Arbeits- und Personalsituation bei kleineren Behörden (z.B. kleinere kreisangehörige Gemeinden) und bei Behörden mit wenigen personenbezogenen Daten Rechnung tragen. Die Kommentarliteratur erwähnt als Beispiel den Fall, dass mehrere öffentliche Stellen über eine gemeinsame Verwaltung verfügen, z.B. wenn ein Zweckverband von einer Gemeinde mitverwaltet wird (Wilde, Ehmann, Niese, Knoblauch, Kommentar und Handbuch zum BayDSG, Art. 25 Rn. 20).

Vom Sinn und Zweck der Vorschrift her scheidet demnach eine gemeinsame Bestellung eines einzigen Datenschutzbeauftragten z.B. für mehrere Städte aus. Eine effektive interne Kontrolle lässt sich insbesondere bei größeren Städten nur durch jeweils einen Datenschutzbeauftragten vor Ort erfüllen.

Ein behördlicher Datenschutzbeauftragter hat eine Vielzahl von gesetzlich vorgeschriebenen Aufgaben zu erledigen:

So haben die behördlichen Datenschutzbeauftragten gemäß Art. 25 Abs. 4 Satz 1 BayDSG die Aufgabe, in ihrer öffentlichen Stelle auf die Einhaltung des BayDSG und anderer Vorschriften über den Datenschutz hinzuwirken. Sie können dazu die erforderliche Einsicht in Dateien und Akten der öffentlichen

Stelle nehmen (Art. 25 Abs. 4 Satz 2 BayDSG). Prüfungsmaßstab ist nicht nur das BayDSG, sondern eine Vielzahl von bereichsspezifischen Normen, wie z.B. SGB X (Sozialgeheimnis), AO (Steuergeheimnis), MeldeG (Meldegeheimnis), BayBG (Personalaktengeheimnis), TKG (Telekommunikationsgeheimnis), TDDSG, BayArchivG, BayEUG, GewO, BSHG, BStatG usw.

Der Datenschutzbeauftragte ist für die gesamte Kommune Ansprechpartner und Auskunftsperson für datenschutzrechtliche Fragen und trägt dazu bei, datenschutzrechtliches Fehlverhalten der Kommune, Haftungsansprüche und ggf. strafrechtlich relevantes (vgl. § 203 Abs. 2 StGB) bzw. ordnungswidriges Verhalten der Beschäftigten zu vermeiden.

Automatisierte Verfahren zur Verarbeitung personenbezogener Daten dürfen nur eingesetzt werden, wenn sie zuvor von dem behördlichen Datenschutzbeauftragten freigegeben worden sind (Art. 26 BayDSG). Das soll sicherstellen, dass in öffentlichen Stellen nur solche automatisierte Verfahren eingesetzt werden, die den Vorschriften des Datenschutzes entsprechen. Die Freigaben sind wegen der notwendigen Abstimmungen (Fachbereiche, EDV-Referat, Personalrat) mit erheblichem Aufwand verbunden. Hinzu kommt die Kontrolle vor Ort, ob die datenschutzrechtliche Freigabe auch eingehalten wird.

Die kommunalen Datenschutzbeauftragten führen ein Verzeichnis aller eingesetzten und datenschutzrechtlich freigegebenen Verfahren ihrer Gemeinde (Art. 27 BayDSG). Dieses Verfahrensverzeichnis kann von jedem kostenfrei eingesehen werden (Art. 27 Abs. 3 Satz 1 BayDSG).

Neben diesen gesetzlich besonders erwähnten Aufgaben sind von den kommunalen Datenschutzbeauftragten weitere Aufgaben auf dem Gebiet des Datenschutzes zu erledigen, z.B. die Beantwortung von Auskunftsersuchen nach Art. 10 BayDSG und von Eingaben von Bürgerinnen und Bürgern, die Beschwerden gegen die Datenverarbeitung der Kommunen erheben (diese können sich auch direkt an die Kommunen wenden).

Diese Aufgaben können wegen der Vielfalt und der Schwierigkeit der Aufgaben von einem einzigen örtlichen Datenschutzbeauftragten für mehrere Städte nicht sach- und zeitgerecht erledigt werden. Diese Schwierigkeiten werden noch potenziert dadurch, dass ein einziger behördlicher Datenschutzbeauftragter noch „fremde“ Städte betreuen und kontrollieren müsste, einschließlich der Einsichtnahme in Datenbestände und Akten auch der anderen Städte. Der Sinn des Gesetzes, nämlich durch die Bestellung eines behördlichen Datenschutzbeauftragten eine ortsnahe Beratung und Kontrolle sicherzustellen, würde durch die Anwendung von Art. 25 Abs. 2 Satz 2 BayDSG auf mehrere Städte in sein Gegenteil verkehrt.

Die Bestellung eines einzigen DSB für mehrere Städte halte ich deshalb für unzulässig. Nachdem ich das den drei Städten mitgeteilt hatte, wurde diese Absicht nicht mehr weiter verfolgt.

22.1.7 Datenarten für die Verfahrensbeschreibung nach Art. 26 Abs. 2 BayDSG sowie Errichtungsanordnung nach Art. 47 Abs. 1 PAG und Art. 9 Abs. 1 Satz 1 BayVSG

Nach Art. 26 Abs. 1 Satz 1 BayDSG bedarf der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, der vorherigen datenschutzrechtlichen Freigabe durch den zuständigen behördlichen Datenschutzbeauftragten. Die personenbezogen Daten können sich auf Bürger, aber auch auf Beschäftigte von Behörden beziehen. Art. 26 Abs. 2 BayDSG zählt den Inhalt einer Verfahrensbeschreibung auf, die die Grundlage der Verfahrensfreigabe bildet.

Zum Kern der Verfahrensbeschreibung gehört die Art der gespeicherten Daten (Art. 26 Abs. 2 Nr. 3 BayDSG). Es genügen aussagefähige **Oberbegriffe und Sammelbezeichnungen** wie Bankverbindungsdaten (= alle Daten, die auf dem Überweisungsträger stehen), Geburtsdaten (= Datum und Ort der Geburt) oder Adressdaten. Die Beschreibung muss aber erkennen lassen, welche Datenarten gespeichert werden. Bei „Antragsdaten“ - z.B. für einen Antrag auf Wohngeld - ist nicht ersichtlich, welche einzelnen Dateninhalte mit dieser Sammelbezeichnung gemeint sind. Im Zweifel sollten die Datenarten daher einzeln aufgeführt werden, wenn dafür keine gängigen und zusammenfassbaren Begriffe gefunden werden können.

Wichtig ist, dass auch für Nichtfachleute nachvollziehbar ist, welche Daten und welcher Dateninhalt gespeichert werden. Es muss ebenso bedacht werden, dass die freigegebenen Verfahrensbeschreibungen für jedermann einsehbar sind (vgl. Art. 27 Abs. 2 BayDSG).

In den Verfahrensbeschreibungen, die für die datenschutzrechtliche Freigabe den behördlichen Datenschutzbeauftragten vorgelegt werden, taucht immer wieder der Begriff **Bemerkung** auf. Dieser Begriff ist zu unbestimmt und nicht eingrenzbar. Er hat keinen Aussagewert über den vorgesehenen Dateninhalt und ist damit als Grundlage für die datenschutzrechtliche Freigabe ungeeignet.

Der Begriff „Bemerkung“ erschwert auch die Arbeit des Sachbearbeiters, der mit dem Programm arbeitet und einerseits nicht weiß, welche Angaben gespeichert werden sollen und andererseits stets im Feld „Bemerkung“ nachsehen muss, ob dort möglicherweise für die aktuelle Bearbeitung relevante Daten enthalten sind.

Für die Daten, die unter „Bemerkung“ gespeichert werden sollen, sind durchaus Alternativen vorhanden, zum Beispiel:

- Hinweise zur Sachbearbeitung
- Stand des Verfahrens/von Eingaben/Petitionen usw.
- Stand von Rechtsbehelfen (Widerspruch/ Klagen)
- Ergebnisse von Vorsprachen, Ferngesprächen oder Besprechungen
- Hinweise zur Bestellung/zur Lieferung/zum Artikel/zur Verteilung usw.
- Schreiben von Antragstellern /Schreiben an Antragsteller (bei Volltextspeicherung)

Der Begriff „Bemerkung“ ist deshalb zur Erläuterung der Datenart ungeeignet und es sollten statt dessen aussagefähigere Bezeichnungen verwendet werden.

22.2 Prüfungen, Beratungen und Informationen

22.2.1 Geprüfte Einrichtungen

Im Berichtszeitraum habe ich bei folgenden Dienststellen die Einhaltung der gebotenen technischen und organisatorischen Datensicherheits- und Datenschutzmaßnahmen überprüft:

- Bayerische Versorgungskammer
- Bezirksklinikum Ansbach
- Bezirkskrankenhaus Landshut
- Bezirksverwaltung Unterfranken in Würzburg
- Große Kreisstadt Nördlingen
- Klinikum Freising
- Kommunaler Eigenbetrieb in Bad Gögging
- Landratsamt Donau-Ries in Donauwörth und Nördlingen
- Landratsamt Regensburg
- Schiller-Gymnasium Hof
- Stadt Regensburg
- Städtisches Krankenhaus Bad Reichenhall
- Städtisches Krankenhaus Landshut
- Virtuelle Hochschule Hof und Bamberg
- Zentrale Aufnahmeeinrichtung für Asylbewerber in Zirndorf

Die Überprüfungen erstreckten sich neben den klassischen Ansätzen der Daten- und Netzwerksicherheit sowie der organisatorischen Aspekte auch auf den datenschutzgerechten Einsatz neuerer Technologien wie Biometrie zur Zugangskontrolle, den Einsatz von Videotechnik und optische Archivierung. Es zeigte sich wie auch in den Vorjahren, dass der Stand der technisch-organisatorischen Maßnahmen zum Teil recht unterschiedlich ist. Wenngleich alle Stellen dem Datenschutz und der Datensicherheit erfreulicherweise einen hohen Stellenwert einräumen wollen, so mangelt es doch gelegentlich an einem umfassenden und schlüssigen Sicherheitskonzept bzw. dessen konsequenter Umsetzung.

22.2.2 Erkenntnisse aus Prüfungen

Aus den vorgenannten Prüfungen ergaben sich wieder eine Reihe von Erkenntnissen bzgl. der praktischen Probleme in der Umsetzung von technisch-organisatorischen Datenschutz- und Datensicherungsmaßnahmen.

Nach wie vor weit verbreitete Mängel bestehen bzgl.

- der Durchführung und der Revisionsfähigkeit der Benutzerverwaltung,
- der Passwortverwaltung,
- der Einbindung des behördlichen Datenschutzbeauftragten,
- der Protokollierung nach Umfang und Speicherdauer,
- der Auswertung von Log-Dateien,
- der Absicherung von Serverräumen und PC-Schnittstellen und
- des Zugriffsschutzes auf schriftliche Unterlagen.

Darüber hinaus zeigten sich noch weit verbreitete Mängel in den nachfolgend ausführlicher beschriebenen Aspekten.

22.2.2.1 Virenbekämpfungskonzept

Während laut neuesten Statistiken (z.B. FBI-Studie aus dem Jahre 2004) Hackerangriffe zurückgehen, waren Viren und andere Formen der Schadenssoftware (Malware) in den letzten Jahren die häufigste Form von Angriffen. Auch der finanzielle Schaden, der durch Viren entstand, war im Jahre 2003 doppelt so hoch wie bei allen anderen Risiken.

Umso erstaunlicher ist die Tatsache, dass es immer noch Behörden gibt, die kein durchgreifendes Virenbekämpfungskonzept erstellt haben. So werden zwar durchaus vereinzelte Maßnahmen wie Installation von Virenscannern auf den Mail-Servern ergriffen, allein es mangelt häufig an einem detaillierten Konzept, das sowohl Sicherheitsrichtlinien in Bezug auf Viren und Maßnahmen zur Verhinderung von Schäden und zur Minimierung des Risikos eines Virenbefalls gegen alle bekannten Arten der Schadenssoftware beinhaltet sowie dabei auch alle IT-Plattformen berücksichtigt. Es genügt eben nicht, nur an einer Stelle Antivirensoftware einzusetzen, sondern dies muss auf allen Ebenen - also sowohl an der Firewall, am Gateway, beim Mail- und Datenbankserver als auch bei den Endgeräten - geschehen. Dieses Sicherheitskonzept und insbesondere seine Regelungen müssen konsequent umgesetzt, laufend überprüft und auch den Bediensteten bekannt sein.

Da ich bereits in meinen letzten Tätigkeitsberichten (z.B. im Kapitel 17.2.1 im 20. Tätigkeitsbericht und im Kapitel 17.1.5 im 19. Tätigkeitsbericht) immer wieder auf die Virenproblematik und mögliche Gegenmaßnahmen hingewiesen habe, will ich im Folgenden nur noch einmal auf einige der wichtigsten Vorsorgemaßnahmen eingehen, die ein Virenkonzept beinhalten sollte:

Über 90 % der Viren, Trojanischen Pferde, Würmer und Backdoor-Programme gelangen heutzutage durch das Einschleusen und Aktivieren von ausführbaren Dateien, etwa mittels E-Mail-Anlage oder beim Besuch einer verseuchten Home-Page im Internet auf die Festplatte eine Rechners oder ins lokale Netzwerk. Ein Anhang (Attachment) einer E-Mail kann nicht nur einen in einer Script-Sprache geschriebenen Virus sondern auch sonstige ausführbare Programme, eine selbstextrahierende Datei oder einen Makrocode (z.B. zur Ausführung in Word-Dokumenten) mit Schadensfunktion enthalten. Deshalb sollten generell nur angeforderte oder erwartete Dateianhänge an E-Mails geöffnet werden. Im Zweifelsfall hilft eine Nachfrage beim Absender weiter, denn auch eine dem Empfänger bekannte Absenderadresse ist kein Indiz für den Erhalt einer virenfreien Mail, da viele Schädlinge Adressen aus den Adressbüchern eines von ihnen befallen Rechners nutzen, um sich weiterzuverbreiten.

Da beispielsweise Script-Viren in E-Mail-Anhängen bereits bei einem Öffnen des Attachments mit Doppelklick aktiviert werden und den Rechner befallen können, sollten Dateianhänge an E-Mails, gleich welcher Art (ob DOC-, VBS-, BAT- oder EXE-Files usw.) keinesfalls mit Doppelklick geöffnet werden, da sonst kein noch so guter Virenschutz greifen kann. Stattdessen rate ich dringend dazu, dass jeder Bedienstete dazu verpflichtet wird, Dateianhänge mit der Funktion „Datei/Anlagen speichern“ auf eine mittels Virenscanner überwachte Festplatte in einem speziell dafür angelegen Verzeichnis zu speichern. Erst dann darf der Dateianhang von der Festplatte aus mit der entsprechenden Anwendung gestartet werden.

Auch bereits das bloße Lesen einer E-Mail im HTML-Format kann das Ausführen eines Codes auslösen, der für eine blitzschnelle Verbreitung des Virus sorgt und/oder eine Schadensfunktion auslöst. Dies kann bereits dadurch geschehen, dass – wie bei den meisten E-Mail-Clients (z.B. Outlook, Outlook-Express oder Netscape Messenger) standardmäßig üblich – ein sogenanntes Vorschaufenster aktiviert ist. Dieses Vorschaufenster öffnet automatisch die erste markierte E-Mail. Befindet sich beispielsweise ein HTML-Virus in dieser markierten E-Mail, so wird er sofort ausgeführt. Deshalb sollte eine Deaktivierung dieser Vorschaufenster erfolgen.

Die gleiche Gefahr besteht beim Herunterladen von Dateien aus dem Internet. Auch sie können Viren enthalten. Deshalb sollte niemals direkt von einer Webseite aus gestartet werden (Funktion „Öffnen“). Stattdessen sollte über die Option „Speichern“ das Programm auf die Festplatte abgelegt und von dort aus geöffnet oder ausgeführt werden. Dabei kann wiederum die heruntergeladene Datei vor dem Starten von einem Virenscanner überprüft werden.

Dies bedeutet natürlich auch, dass der Virenscanner stets aktiv im Hintergrund laufen muss. Wird er deaktiviert, kann er verdächtige Dateien nicht erkennen.

Eine wichtige Maßnahme besteht darin, das auf dem Rechner installierte Antivirenprogramm durch möglichst tägliche Updates der Virensignaturen (=Datenbank mit Informationen zu den Schädlingen) immer auf dem neuesten Stand zu halten, denn ein nicht aktualisierter Virenscanner ist schlimmer als kein Virenscanner, da dem Anwender eine Sicherheit vorgegaukelt wird, die in Wirklichkeit nicht vorhanden ist.

Selbstverständlich sollte auch sein, dass alle Software auf Viren geprüft wird, bevor sie im Netzwerk installiert wird.

Immer mehr Schadenssoftware (insbesondere Würmer und Trojanische Pferde) nutzen zu ihrer Verbreitung Sicherheitslücken in Browsern und Betriebssystemen aus. Deshalb sollten immer aktuelle Patches, Bugfixes und Programm-Updates der Softwarehersteller eingespielt werden. So bringt etwa die Firma Microsoft einmal monatlich, in der Regel an jedem zweiten Mittwoch eines Monats, Windows-Updates heraus, die sicherheitskritische Fehler beheben.

Viele Softwarehersteller haben in ihren Produkten eine Update-Funktion integriert, die automatisch in definierten Zeiträumen auf den Home-Pages dieser Anbieter nach dem Vorhandensein neuer Programmkomponenten zur Fehlerbereinigung sucht. Dazu nehme ich aber eine kritische Haltung ein (vgl. Nr. 22.3.4).

22.2.2.2 Online-Datenschutz-Prinzipien

Die Veröffentlichung von Informationen auf einer Home-Page und das Bereitstellen von Angeboten, z.B. in Form von Formularen u.ä., ist als ein Teledienst im Sinne des § 2 Abs. 2 Teledienstegesetz (TDG) anzusehen. Somit sind auch bezüglich des Internetauftritts (Home-Page) öffentlicher Stellen sowohl die Vorschriften des TDG als auch die des Teledienstedatenschutzgesetzes (TDDSG) zu beachten.

Gemäß § 4 Abs. 1 Teledienstedatenschutzgesetz (TDDSG) muss der Diensteanbieter den Nutzer des Teledienstes (z.B. den Besucher der Home-Page) zu Beginn des Nutzungsvorganges über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten unterrichten. Der Diensteanbieter muss darüber informieren, welche Arten von Daten erhoben, verarbeitet und genutzt werden, für welche Zwecke dies erfolgt, wo und wie lange sie gespeichert und eventuell an wen sie weitergegeben werden. Dies geschieht mit Hilfe so genannter Online-Datenschutz-Prinzipien (Privacy Policy).

Die Erhebung personenbezogener Daten im Zusammenhang mit einem Internetauftritt beginnt grundsätzlich dann, wenn der Nutzer ein Web-Angebot aufruft, denn dabei werden die IP-Adresse des vom Nutzer verwendeten Rechners und weitere technische Angaben automatisch an den Anbieter weitergeleitet. Auch eine bei einer Einwahl ins Internet über einen Internet-Provider vergebene temporäre IP-Adresse, die zufällig aus einem Pool an freien IP-Adressen ausgewählt und einmalig für die Zeit der Online-Verbindung einem PC zugeordnet wird, besitzt einen Personenbezug, da der Provider natürlich die Vergabe der IP-Nummern für einen begrenzten Zeitraum zum Beispiel zur Kostenabrechnung speichern muss. Damit ist über den Provider auch wieder der temporäre Besitzer dieser IP-Adresse ermittelbar.

Spätestens zu dem Zeitpunkt, wenn der Nutzer zur Angabe persönlicher Daten aufgefordert wird (z.B. Ausfüllen eines Online-Formulars oder Beginn einer Kommunikation mittels E-Mail) oder wenn Dateien mit direktem oder indirektem Personenbezug von seinem Rechner abgerufen werden, die dort schon gespeichert vorliegen (etwa in so genannten Cookies), muss der Diensteanbieter den Nutzer unterrichten. Die Unterrichtung muss vollständig und verständlich sein. Diese Unterrichtung bzw. der Hinweis auf die Unterrichtung ist so anzubringen, dass ein Nutzer sie üblicherweise zur Kenntnis nimmt, wenn er das entsprechende Angebot aufruft. Verstöße gegen diese gesetzlich geforderten Informationspflichten sind als Ordnungswidrigkeiten zu betrachten, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden können.

Umso verwunderlicher ist es, dass ich im Rahmen meiner Prüfungen feststellen musste, dass kaum eine der geprüften Stellen eine gesetzeskonforme Online-Datenschutzerklärung erstellt hatte. Dabei habe ich bereits sowohl in Kapitel 17.4 meines 19. Tätigkeitsberichts als auch in Kapitel 17.1.7 meines 20. Tätigkeitsberichts auf diese Informationspflichten hingewiesen.

Nähere Hinweise zu den Online-Datenschutz-Prinzipien enthält meine gleichnamige Orientierungshilfe – abrufbar auf meiner Home-Page (www.datenschutz-bayern.de) im Bereich „Technik/ Grundsätze“.

22.2.2.3 Anbieterkennzeichnung

Neben einer Online-Datenschutzerklärung muss jeder Betreiber einer Home-Page, der Waren oder **Dienstleistungen** anbietet, seine Home-Page auch mit einer Anbieterkennzeichnung (Impressum) gemäß § 6 Teledienstegesetz (TDG) ausstatten. Gleiches gilt gemäß § 10 Mediendienste-Staatsvertrag (MDStV) für die Anbieter von Seiten redaktionellen Inhalts.

Die Anbieterkennzeichnung soll für den Nutzer ein Mindestmaß an Transparenz und Information über die natürliche oder juristische Person oder Personengruppe, die ihm beispielsweise einen Teledienst anbietet, sicherstellen. Die Informationen zur Anbieterkennzeichnung müssen an gut wahrnehmbarer Stelle und ohne langes Suchen und jederzeit auffindbar sein. Es darf also nicht der Fall sein, dass ein Besucher der Home-Page die Anbieterkennzeichnung erst durch so genanntes „Scrollen“ (Vorwärtsblättern) einen Hinweis auf das Impressum findet. Die Anbieterkennzeichnung darf auch nicht in Allgemeinen Geschäftsbedingungen „versteckt“ sein. Außerdem muss die Anbieterkennzeichnung z.B. mittels Link von jeder Seite der Home-Page aufrufbar sein. Dieser Link sollte zur Verdeutlichung mit Anbieterkennzeichnung oder Impressum tituliert sein.

Die verantwortliche Person des Diensteanbieters (in der Regel der Bürgermeister oder Dienststellenleiter) trägt die volle Verantwortung für die Inhalte seiner Home-Page. Dies gilt auch für den Fall, dass der

Anbieter von Inhalten die technische Abwicklung seines Dienstes einem Dritten überträgt (so genanntes Web-Hosting).

Die Pflicht zur Angabe von Identität und Anschrift dient auch als Anknüpfungspunkt für die Rechtsverfolgung in einem Streitfall. Deshalb muss die Information so vollständig sein, dass sie quasi als ladungsfähige Adresse für einen Rechtsstreit geeignet ist.

Bei öffentlichen Stellen sind auf ihrer Home-Page folgende Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar anzubringen:

- Der Name und die Anschrift der Dienststelle
- Der Vor und Nachname des Verantwortlichen (z.B. der Dienststellenleiter)
- Die vollständige Postanschrift und sonstige Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post

Bei fehlenden Anbieterkennzeichnungen oder fehlerhaften Angaben zur Anbieteridentität können wiederum Bußgelder in Höhe von bis zu 50.000 Euro verhängt werden.

22.2.2.4 Sonstige Erkenntnisse

Reaktion der IT-Systeme auf Anmeldefehlversuche

Obwohl alle modernen Betriebssysteme über die Möglichkeit verfügen, fehlerhafte Anmeldeversuche abzuweisen und zu sanktionieren, wird davon immer noch bei vielen öffentlichen Stellen nicht Gebrauch gemacht. Ich weise daher erneut darauf hin, dass nach höchstens fünfmaliger fehlerhafter Anmeldung in ununterbrochener Reihenfolge bei allen IT-Systemen der Anmeldedialog abgebrochen und das entsprechende Endgerät „out of service“ gesetzt bzw. die betreffende Benutzerkennung auf Dauer gesperrt werden muss, damit etwaige missbräuchliche Zugriffsversuche unterbunden werden. Eine Entsperrung sollte nur durch eine dazu berechtigte Person (z.B. Systemverwalter) möglich sein. Den Ursachen für fehlerhafte Anmeldeversuche ist nachzugehen.

Datenschutzmaßnahmen für mobile Rechner

Mobile Computer stellen aufgrund ihrer Mobilität und geringen Größe ein besonderes Sicherheitsrisiko dar, da für sie eine erhöhte Gefahr bezüglich eines Diebstahls oder eines Verlusts besteht. Auf diesen Geräten können genauso vertrauliche Informationen gespeichert werden, wie bei einem stationären Gerät. Insbesondere die Speicherung personenbezogener Daten auf einem PDA ist besonders gefährlich, da PDAs standardmäßig keinerlei Maßnahmen zur Gewährleistung des Zugangsschutzes (insbesondere keinen Boot-Schutz) und der Vertraulichkeit bieten. Der einzige Zugangsschutz besteht in der Regel darin, die Eingabe eines höchstens vierstelligen Passworts zu erzwingen. Soweit keine weiteren Maßnahmen ergriffen werden, sind damit natürlich die Anforderungen des Datenschutzes nicht erfüllt.

Daher ist die verschlüsselte Speicherung von personenbezogenen Daten auf Datenträgern in mobilen Rechnern (z.B. Laptops, Notebooks, PDA) sowie die Ergreifung datenschutzgerechter Maßnahmen zur Gewährleistung der Zugangs- und Zugriffssicherheit unbedingt erforderlich, damit die Daten bei einem Verlust oder Diebstahl des Rechners nicht in unbefugte Hände geraten. Dazu ist in der Regel der Einsatz entsprechender Zusatzsoftware erforderlich.

Möglichst kein Versenden von Telefaxen mit personenbezogenem Inhalt

Da Verschlüsselungstechniken bei einem Telefax-Versand – ob konventionell oder auch mittels PC - aufgrund des verwendeten Protokolls derzeit nicht zur Verfügung stehen, sollte zur Gewährleistung der Vertraulichkeit – außer wenn dadurch in einem Notfall eine nicht zumutbare Zeitverzögerung entstehen würde – ein Versand sensibler personenbezogener Daten per Telefax unterbleiben. Zu den zu ergreifenden Sicherheitsmaßnahmen habe ich mich in Kapitel 17.2.2 meines 19. Tätigkeitsberichts bereits geäußert und weise auch auf meine Orientierungshilfe „Datensicherheit beim Telefax-Dienst“ hin, die auf meiner Home-Page unter www.datenschutz-bayern.de/technik/orient/telefax.htm zu finden ist.

Sichere Browserkonfiguration

Viele Dienststellen gestatten zwar ihren Mitarbeitern das Surfen im Internet, vergessen aber dabei, entsprechende Sicherheitseinstellungen bei den eingesetzten Web-Browsern zu nutzen. Ich rate dringend dazu, die Sicherheitseinstellungen der Browser zu aktivieren und den Bedürfnissen anzupassen (z.B. beim Internet Explorer unter Extras / Internetoptionen / Sicherheit). Dadurch lässt sich die Sicherheit im Internet beträchtlich steigern. Insbesondere sollten – soweit nicht unbedingt erforderlich – die Ausführung von ActiveX-, Java- und Javascript-Programmen durch Browser-Einstellungen abgeschaltet oder nur nach automatischer Rückfrage gestattet werden. Auch die AutoVervollständigen-Funktion der Browser, wodurch die Eingaben von Benutzerkennungen und Passworten gespeichert werden, sollte nicht genutzt werden. Bei den meisten Browsern kann vordefiniert werden, ob ein Benutzer die Sicherheitseinstellungen

ändern darf oder nicht. Soweit möglich, sollte eine Änderungsmöglichkeit durch den Benutzer unterbunden werden.

Mit Hilfe eines **Online-Checks** können Personal Computer auf sichere Browser-Einstellungen und mögliche Sicherheitslücken hin überprüft werden. Auch ein Port-Scan sollte im Rahmen des Online-Checks durchgeführt werden. Dabei wird festgestellt, welche Internetdienste auf dem PC aktiv sind und welche Ports sie belegen. Werden bei dieser Überprüfung Ports als Offen bezeichnet, bedeutet dies eine potenzielle Hintertür für das Eindringen von Hackern oder Trojanischen Pferden. Deshalb führen auch Hacker, die versuchen wollen, in einen Rechner oder in ein Netzwerk einzudringen, zunächst einen Port-Scan durch, um einen offenen Port zu finden. Nach Abschluss der Tests sollten Erkenntnisse über den Sicherheitsstatus des PC vorliegen. Zusätzlich geben viele Checks Hinweise auf angemessene Sicherheitseinstellungen sowie Tipps für weiter gehende Informationen über mögliche Gefahren und deren Vermeidung.

Entsprechende Selbsttests können auf verschiedenen Webseiten (z.B. beim Landesbeauftragten für den Datenschutz Niedersachsen: www.lfd.niedersachsen.de) abgerufen werden. Grundsätzlich sollte darauf geachtet werden, dass Eingaben und Ergebnisse immer verschlüsselt übertragen werden. Ich weise aber deutlich darauf hin, dass in den Fällen, in denen eine Firewall den zu testenden Rechner gegen das Internet oder andere Netze schützt, diese Tests natürlich nur auf die Firewall wirken, d.h. diese getestet wird, und der Test dort evtl. als Angriff gewertet wird. Solche Tests sollten also nur von hierzu berechtigten Systemadministratoren und nicht von „Normal-Nutzern“ von innerhalb eines lokalen Netzwerkes angestoßen werden.

Da bekanntermaßen gerade der Internet Explorer gerne Angriffsziel ist, sollte der Einsatz alternativer Browser zumindest bedacht werden.

22.2.3 Beratungsleistungen

Auch in diesem Berichtszeitraum ist die Zahl der Nachfragen nach Beratungsleistungen stark angestiegen und nahm im technisch-organisatorischen Bereich einen ganz wesentlichen Teil meiner personellen Kapazitäten in Anspruch. Diesen Anfragen komme ich, soweit personell und zeitlich möglich, gerne nach. Darauf bin ich bereits in meinem letzten Tätigkeitsbericht eingegangen (Kapitel 17.2.2 im 20. Tätigkeitsbericht).

Ich möchte diese Gelegenheit nutzen, mein vielfach geäußertes Angebot nach Vorab-Beratung auch an dieser Stelle zu wiederholen und alle Dienststellen zu ermuntern, bereits im Vorfeld von Neu-Einführungen oder gravierenden Änderungen an ihren IuK-Systemen um Beratungsleistung zunächst des behördlichen Datenschutzbeauftragten nachzufragen. Durch die frühzeitige Einbindung des behördlichen Datenschutzbeauftragten einerseits und sodann meiner Dienststelle andererseits können eventuell aufwändige Nachbesserungen an Systemen und Abläufen vermieden werden – von Verletzungen der Datenschutzvorschriften im Wirkbetrieb ganz abgesehen.

Auf einige der Projekte, die ich beraten habe, bin ich in den Kapiteln „TEMPiS“ (vgl. Nr. 5.1) und „Gesundheitsmodernisierungsgesetz und elektronische Gesundheitskarte“ (vgl. Nr. 6.1) bereits eingegangen. Auf einige weitere Projekte möchte ich im Folgenden näher eingehen.

22.2.3.1 KVB Safenet

In zunehmendem Maße steigen auch im Bereich der niedergelassenen Ärzte die Anforderungen an die medizinische Dokumentation, was z.B. die Vollständigkeit, Fehlerfreiheit und Qualität der erfassten Daten betrifft. Gleichzeitig nimmt die Verbreitung standardisierter Programme zur Versorgung von Patienten zu, z.B. im Rahmen von Disease Management Programmen, die ebenfalls eine sorgfältige Dokumentation erfordern. Auch der Wunsch nach einer Erhöhung der Effizienz der Datenerfassung und Verarbeitung führt zunehmend in Richtung der medienbruchfreien elektronischen Erhebung von medizinischen Daten. Ein geeigneter Lösungsansatz hierfür ist die Bereitstellung von Web-Portalen, auf denen die behandelnden Ärzte direkt über einen Web-Browser an ihrem Praxis-PC die Patientendaten eingeben können. Voraussetzung ist allerdings, das mindestens ein Praxiscomputer eine Außenanbindung besitzt, mit der der Dokumentationsserver angesprochen werden kann.

Die Kassenärztliche Vereinigung Bayerns (KVB) bietet mit dem KVB Safenet hierzu eine Basisinfrastruktur für die bayerischen Kassenärzte. Aufbauend auf einer gesicherten Vernetzungsinfrastruktur soll eine Online-Dokumentation für verschiedene Programme wie z.B. das Mammographie-Screnning (vgl. Nr. 6.2) möglich sein. Die Anbindung der Ärzte erfolgt über ein VPN, das derzeit auf ISDN und einem gesonderten Netz eines Providers basiert, in Zukunft aber auch via DSL über das Internet laufen soll. Zur Teilnahme müssen die Ärzte ihr Praxissystem mit einem gemäß den Sicherheitsrichtlinien der KVB vorkonfigurierten ISDN-Router ausstatten, der den Zugang zum VPN und auf die von der KVB bereitgestellten Web-Portale möglich macht.

Da bei dieser Art von medizinischer Dokumentation personenbezogene medizinische Daten an Stellen außerhalb der Arztpraxis übermittelt und dort gespeichert werden, spielen Datenschutz sowie technisch-organisatorische Sicherheit im Projekt eine große Rolle. Daher wurde ich beratend von der KVB hinzugezogen. Es ergeben sich aus Datenschutzsicht für derartige Konzepte diverse Anforderungen, die einerseits den Schutz der Praxissysteme und des KVB Safenet-Zugangs des niedergelassenen Arztes, andererseits die Datenübertragung sowie die Speicherung der Daten auf den Servern der KVB betreffen.

- **Schutz der Praxissysteme:** Praxis-Computer, die an das KVB Safenet angeschlossen werden, dürfen nicht mit einem Internetzugang ohne zusätzliche Schutzmaßnahmen wie z.B. Firewalls ausgestattet sein, da sonst ein Einbruch in das KVB Safenet aus dem Internet möglich wäre. Analoges gilt für alle Praxis-Rechner, auf denen personenbezogene Patientendaten gespeichert werden, da hier ein unerwünschter Zugriff auf die gespeicherten Daten erfolgen könnte. Daher ist für eine Internetnutzung der Einsatz eines gesonderten PCs, der keine Verbindung zu den sonstigen Praxis-PCs hat, erforderlich.

- **Verbindungsaufbau zum KVB Safenet und Zugang zum Web-Portal:** Es muss über personenbezogene Kennungen und Passworte / Chipkarten o.ä. sichergestellt werden, dass nur teilnehmende Ärzte auf das KVB Safenet und das Web-Portal zugreifen können. Insbesondere darf der Arzt die entsprechenden Zugangsinformationen nicht weitergeben. Regeln zur Gestaltung sicherer Passworte finden sich z.B. auf meiner Home-Page unter www.datenschutz-bayern.de/technik/orient/pwreg.htm.
  Zudem muss mittels der Benutzerkennungen dafür gesorgt werden, dass jeder Arzt nur auf die von ihm erhobenen Daten zugreifen kann.

- **Einschränkung der Verbindungsmöglichkeiten:** In den teilnehmenden Arztpraxen (ISDN-Router) und auf Seiten der KVB sollte durch eine entsprechende Konfiguration der Netzzugänge und eine Überprüfung von Verbindungsaufbauwünschen sichergestellt werden, dass sowohl ein- als auch ausgehende Verbindungen nur von und zu festgelegten Stellen möglich ist. Damit wird z.B. verhindert, dass aus der Arztpraxis unerwünschterweise eine andere Stelle für einen Datenexport angewählt wird oder dass Nichtbeteiligte eine Verbindung zum Web-Portal der KVB aufbauen können.

- **ISDN Sicherheitsmechanismen:** Bei einer Datenübermittlung über ISDN sollten die von ISDN angebotenen Sicherheitsmechanismen wie geschlossene Benutzergruppe, Rufnummernidentifizierung / Teilnehmerauthentifizierung und Callback-Mechanismen zum Einsatz kommen, um einen Verbindungsaufbau von und zu unerwünschten Partnern zu verhindern.

- **Verschlüsselte Datenübertragung:** Zum Schutz vor unbefugter Kenntnisnahme sollte eine verschlüsselte Datenübertragung erfolgen. Zwingend erforderlich ist dies, wenn medizinische Daten über das Internet übermittelt werden, wie es z.B. bei der geplanten Anbindung über DSL der Fall ist.

- **Fernwartung:** Grundsätzlich muss sichergestellt werden, dass im Falle einer Bereitstellung von Endgeräten durch Dritte oder im Rahmen von Wartungsverträgen keine unbefugte Kenntnisnahme der Daten durch den die Wartung Durchführenden stattfindet. Dies betrifft z.B. den ISDN-Router in der Arztpraxis. Es muss durch eine entsprechende Konfiguration und organisatorische Maßnahmen (Verpflichtung der Mitarbeiter, Trennung der Aufgaben etc.) dafür gesorgt werden, dass die Wartungsfirma über den Router keinen Zugriff auf das Praxissystem erhält.

- **Schutz des Web-Portals und der Datenbank:** Wie die Systeme in der Arztpraxis müssen auch die Server des Web-Portals sowie die Datenbank zur Speicherung der Erfassungsbögen über eine Firewall vor unbefugtem Zugriff durch Hacker oder Schadenssoftware geschützt werden.

- **Interne Anbindung von Web-Portal und Datenbank:** Es sollte darauf geachtet werden, dass auch innerhalb der KVB bzw. des Web-Portal-Providers der Zugriff auf den Web-Server und die Datenbank nur für Berechtigte möglich ist. Dies kann z.B. dadurch erreicht werden, dass eine physikalische Trennung von den sonstigen Systemen vorgenommen wird oder durch die Zwischenschaltung von Firewalls.

- **Datenbankzugriff:** Für den Zugriff berechtigter Personen auf die Daten der Datenbank müssen personenbezogene Kennungen und sichere Authentifizierungsmaßnahmen genutzt werden. Nur so kann verhindert werden, dass z.B. Mitarbeiter der KVB, die nichts mit dem in der Datenbank erfassten Behandlungsprogramm zu tun haben, Kenntnis von den ge-

speicherten Daten erlangen. Die berechtigten Personen sind für das jeweils auf dem KVB Safenet eingesetzte Programm, z.B. Mammographie-Screening, DMP Diabetes, gesondert zu definieren und in ein Berechtigungskonzept für die Datenbanknutzung umzusetzen.

- **Administratorenrechte:** Häufig besteht die Gefahr, dass Systemadministratoren im Rahmen ihrer Tätigkeit Kenntnis von den gespeicherten Daten erhalten. Dem kann zum einen durch eine verschlüsselte Datenspeicherung begegnet werden. Zum anderen ist es sinnvoll, verschiedene Administratorrollen mit unterschiedlichen Rechten und Aufgaben zu definieren, damit nicht eine Person Zugriff auf alle Informationen und Systeme hat.

- **Protokollierung:** An diversen Stellen sollte eine Protokollierung der Vorgänge erfolgen, um die Revisionsfähigkeit und Überprüfbarkeit von Zugriffen und Aktionen zu gewährleisten. Dies betrifft z.B. die Fernwartung auf dem ISDN-Router oder unbefugte Zugriffsversuche und Änderungen an der Dokumentation auf dem Webportal. Auch die Protokollierung von Administratorzugriffen kann sinnvoll sein.

- **Nutzung der Daten:** Es muss festgelegt werden, zu welchem Zweck und durch wen eine Weiterverarbeitung der in der Datenbank gespeicherten Daten erfolgen darf. Anschließend müssen angemessene technische und organisatorische Maßnahmen getroffen werden, die eine unbefugte Nutzung verhindern. Auch für eine eventuelle weitere Datenübertragung, z.B. zu den Krankenkassen, sind Schutzmaßnahmen nötig.

22.2.3.2 Verschlüsselte Datenarchivierung bei externen Providern

Die zunehmende Digitalisierung spielt in vielen Bereichen, so auch im Gesundheitswesen eine immer stärkere Rolle. Mit ihr steigt die Zahl der über längere Zeiträume zu archivierenden elektronischen Dokumente. Im Krankenhaus können beispielsweise Aufbewahrungszeiten von bis zu 30 Jahren für Röntgenbilder verpflichtend sein. Es ist einsichtig, dass hier eine große Menge von Daten mit hohem Aufwand und Sachverstand gelagert, gepflegt und zugänglich gehalten werden muss, der die Kapazitäten des Krankenhauses in erheblichem Maße bindet. Deshalb streben vermehrt Krankenhäuser die Nutzung externer Provider für die Archivierung der Daten an. Da es sich zumeist um personenbezogene medizinische Daten handelt, für die nach dem Bayerischen Krankenhausgesetz besondere Schutzvorschriften gelten, sind derartige Vorhaben technisch wie juristisch besonders sorgfältig zu bewerten.

Basis der folgenden Darstellung ist eine im Berichtszeitraum vorgenommene Bewertung einer Gesamtlösung zur längerfristigen externen Archivierung von Röntgendaten. Bei dieser Lösung sollen nicht mehr benötigte Bilder nach 4 Jahren in verschlüsselter Form zu einem externen Provider ausgelagert und lokal gelöscht werden. Bei Bedarf soll ein Reimport der Daten möglich werden. Hierzu werden die bildgebenden Systeme an einen speziellen Server, der sich in den Räumen des Krankenhauses befindet, angeschlossen. Auf diesem Server werden zunächst die Daten abgelegt und genutzt. Für die Archivierung besitzt dieser Server eine Anbindung an das externe Rechenzentrum, wo für jeden Kunden eine eigene Datenbank vorhanden ist. Zum Schutz vor Datenverlust werden die Daten zudem auf Bändern gespeichert und an verschiedenen Orten gelagert. Sollen Daten aus dem Kliniksystem archiviert werden, werden sie vom Server verschlüsselt, wobei der geheime Schlüssel passwortgeschützt auf einem speziellen USB-Stick (eToken) gespeichert ist, und anschließend zum Provider übertragen. Um auch bei einem Verlust des USB-Sticks noch auf die Daten zugreifen zu können, erhält der Kunde zusätzlich eine Sicherungskopie, die sicher verwahrt werden muss.

In rechtlicher Hinsicht habe ich auf Folgendes aufmerksam gemacht:

Bei den Vorhaben sind in erster Linie die Vorgaben des Bayerischen Krankenhausgesetzes zu beachten.

1. Bei den Röntgenbildern handelt es sich um **Patientendaten**. Im Archiv werden Bilddaten (z.B. Röntgenbilder, Durchleuchtungen, Sonographien, nuklearmedizinische Bilder) und Befunde des Arztes mit dem Namen zwar verschlüsselt abgelegt und der Personenbezug ist nur mit Zusatzwissen (Kenntnis des Schlüssels) herstellbar. Jedoch ist das Klinikum in Besitz des Schlüssels, sodass es sich für das Klinikum um personenbezogene Daten handelt.

2. Das Gesetz differenziert zwischen Patientendaten, die zur verwaltungsmäßigen Abwicklung erforderlich sind und solchen, die dies nicht sind. Bei Letzteren, nämlich den hier vorliegenden medizinischen Daten, ist das Datenschutzniveau angehoben, da die Auftragsdatenverarbeitung nach Art. 27 Abs. 5 Satz 6 Bayerisches Krankenhausgesetz (BayKrG) nur in einem anderen Krankenhaus erfolgen darf. Dies wäre in dem mir vorlie-

genden Fall nicht gegeben gewesen. Es stellte sich daher die Frage, ob der Gesetzeswortlaut so ausgelegt werden kann, dass auch die externe Archivierung durch Private darunter gefasst werden kann. Deshalb war nach Sinn und Zweck der Regelung des Art. 27 Abs. 5 Satz 6 BayKrG zu fragen. Hier sind zwei Aspekte zu unterscheiden. Zum einen sollte durch die Norm der Beschlagnahmeschutz gewährleistet sein, zum anderen sollte der Kreis der Personen, die mit Patientendaten in Berührung kommen, möglichst eng und qualifiziert sein.

a) Für Daten, die nicht zur verwaltungsmäßigen Abwicklung erforderlich sind („medizinische Daten"), sollte der Beschlagnahmeschutz des § 97 Abs. 2 StPO a.F. gewährleistet werden. Denn früher mussten sich die Datenträger im Gewahrsam des Krankenhauses befinden, um „beschlagnahmefest" zu sein. Diese gesetzgeberische Intention des BayKrG ist mittlerweile durch eine Gesetzesnovellierung des § 97 Abs. 2 StPO erfüllt. Durch Art. 30 Nr. 2 des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz-GMG, BGBl 2003 Teil I, Seite 2190 ff., 2256) hat § 97 Abs. 2 Satz 2 der Strafprozessordnung (StPO) mit Wirkung ab dem 01.01.2004 (Art. 37 Abs. 1 GMG) folgende Fassung erhalten:

„Der Beschlagnahme unterliegen auch nicht Gegenstände, auf die sich das Zeugnisverweigerungsrecht der Ärzte, Zahnärzte, Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen erstreckt, wenn sie im Gewahrsam einer Krankenanstalt **oder eines Dienstleisters, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt**, sind, sowie Gegenstände, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 3 a und 3 b genannten Personen erstreckt, wenn sie im Gewahrsam der in dieser Vorschrift bezeichneten Beratungsstelle sind."

Mit der Neuregelung wird damit der Schutz dieser Daten über den Gewahrsam eines Krankenhauses hinaus erweitert auf den Gewahrsam eines Datenverarbeiters im Auftrag der Genannten.

b) Damit gefährdet ein fehlender Beschlagnahmeschutz das Recht auf informationelle Selbstbestimmung nicht mehr. Die gesetzgeberische Regelung kann nur noch den Sinn haben, dass der Kreis der Personen, die mit medizinischen Daten in Berührung kommen, möglichst eng und qualifiziert sein soll. Unbefugte sollen von medizinischen Daten keine Kenntnis erhalten. Dies hielt der Gesetzgeber in Krankenhäusern wohl eher für gewährleistet als außerhalb.

Dieser gesetzgeberische Zweck ist jedoch unter bestimmten Voraussetzungen auch dann erfüllt, wenn die Daten verschlüsselt bei einem Auftragnehmer gespeichert werden. Durch bestimmte technische Maßnahmen können die Gefährdungen für das Recht auf informationelle Selbstbestimmung minimiert werden. Dabei kann zwar nicht generell jegliche Gefährdung ausgeschlossen und von garantierter Sicherheit in jedem Fall gesprochen werden. Entscheidend ist insofern, dass bei den technischen und organisatorischen Maßnahmen ein Standard erreicht wird, der die **praktische** Sicherheit des Verfahrens gewährleistet. Hierzu sind sowohl vom Systemanbieter als auch vom Klinikum gewisse technisch-organisatorische Aspekte der Realisierung zu untersuchen und Anforderungen zu erfüllen.

Dies beinhaltet mehrere Aspekte, die in unterschiedliche Verantwortlichkeiten fallen. Die im Folgenden aufgeführten Punkte 1. und 2. müssen vom Systemanbieter sichergestellt werden, für die Punkte 3. und 4. sind Anbieter und Krankenhaus gemeinsam verantwortlich und 5. liegt vor allem in der Zuständigkeit des Krankenhauses.

1. Theoretische Sicherheit des Verschlüsselungsverfahrens
2. Praktische Nichtangreifbarkeit des Verschlüsselungsverfahrens
3. Unterbindung unbefugter Entschlüsselungsversuche mit Zusatzwissen
4. Sichere Installation und Initialisierung des Systems
5. Gewährleistung einer gesicherten Einsatzumgebung

Zu 1. Theoretische Sicherheit des Verschlüsselungsverfahrens:

Es muss sichergestellt werden, dass nur Verschlüsselungsverfahren zum Einsatz kommen, die veröffentlicht sind und daher von anerkannten Experten kyptanalytisch untersucht wurden. Nur so kann sichergestellt werden, dass das eingesetzte Verfahren ein nach dem derzeitigen Wissensstand starkes Verschlüsselungsverfahren ist, das keine Einbruchsmöglichkeiten bietet. Auch die Angaben zur momentan geeigneten Mindestschlüssellänge sind zu befolgen. Es ist sicherzustellen, dass schwache Schlüssel, soweit vorhanden, nicht verwendet werden.

Zu 2. Praktische Nichtangreifbarkeit des Verschlüsselungsverfahrens:

Häufig beruht eine praktische Angreifbarkeit von theoretisch sicheren Verfahren auf Fehlern bei der Implementierung. Hierzu gehört z.B. ein schlecht programmierter Zufallszahlengenerator, der zur Schlüsselerzeugung benötigt wird. Ein solcher Zufallszahlengenerator ist unter Umständen vorhersagbar oder erzeugt nur einen Teil der theoretisch möglichen Schlüssel. Damit kann der Schlüsselraum deutlich eingeschränkt werden, sodass z.B. bei symmetrischen Verfahren, für die heute im allgemeinen 128 Bit als ausreichende Schlüssellänge angesehen werden, die Zahl der auszuprobierenden Kombinationen so weit gesenkt werden kann, dass ein Brute Force Angriff realistisch erscheint.

Zu 3. Unterbindung unbefugter Entschlüsselungsversuche mit Zusatzwissen:

Häufig stützen sich kryptanalytische Methoden auf Zusatzinformationen, die dem Angreifer neben dem verschlüsselten Text zur Verfügung stehen. Solche Informationen können gerade einem internern Angreifer zugänglich sein, wie z.B. den Administratoren des Rechenzentrums. Es muss daher durch geeignete organisatorische Maßnahmen ausgeschlossen werden, dass ein interner Angreifer einerseits zu viele Informationen, andererseits Zugang zu den verschlüsselten Daten erhalten kann, um unbefugte Entschlüsselungsversuche zu unternehmen:

Durch Rollentrennung ist auszuschließen, dass ein Mitarbeiter sowohl Entwickler als auch Anwender (z.B. Wartungstechniker) des Verfahrens oder Administrator ist. Damit soll verhindert werden, dass einerseits der Entwickler Zugriff auf Echtdaten erhält und andererseits der Anwender Zugriff auf den Quellcode und der Administrator Zugang zur Verschlüsselungssoftware hat. Auch der Zugriff auf die verschlüsselten Daten sowie Kenntnisse zur Erzeugung des Schlüssels und Zugang zur Software, die den Schlüssel generiert, dürfen nur einem möglichst kleinen Kreis zugänglich sein.

Die Schutzfunktion von Verschlüsselungsverfahren ist zeitlich begrenzt. Dies kann sowohl die Schlüssellänge, als auch das gesamte Verfahren betreffen, wenn sich mit dem technischen Fortschritt die verfügbare Rechenleistung erhöht oder neue Erkenntnisse im Bereich der Kryptanalyse bekannt werden. Um die Sicherheit der Daten über 30 Jahre hinweg zu erhalten, wird ein Verfahren benötigt, das die archivierten Daten bei Bedarf verschlüsselungstechnisch auf den neuesten Stand bringt. Für die Krankenhausmitarbeiter muss während dieser Umschlüsselung durch den Anbieter überprüfbar sein, dass kein unbefugter Zugriff auf die unverschlüsselten Daten erfolgt. Im Rechenzentrum muss gleichzeitig sichergestellt werden, dass die alten Datenbestände auch wirklich gelöscht werden.

Zu 4. Sichere Installation und Initialisierung des Systems:

Im Rahmen der Systeminstallation im Krankenhaus muss einerseits sichergestellt werden, dass die Techniker des Anbieters keine Kenntnisse von den personenbezogenen medizinischen Daten erlangen. Andererseits darf ein Techniker keinen Zugriff auf den Verschlüsselungsschlüssel, den er erzeugt, erhalten. Zusätzlich sollte er möglichst wenig Kenntnisse über das Verfahren zur Erzeugung des Schlüssels haben. Darüber hinaus muss bei Wartungs- und Fernwartungsarbeiten gewährleis-

tet sein, dass der Techniker auch hier keine Einsicht in die Daten auf dem Server im Krankenhaus oder den Schlüssel erhält.

Zu 5. Gewährleistung einer gesicherten Einsatzumgebung:

Die Sicherheit des Gesamtsystems ist nicht ausschließlich abhängig von der Verschlüsselung der ausgelagerten Bilddaten. Das Krankenhaus muss zudem für eine geschützte Einsatzumgebung sorgen:

Der Verschlüsselungsschlüssel wird im Rahmen der Systeminstallation auf einem passwortgeschützten USB-Stick gespeichert. Das Krankenhaus muss darauf achten, dass die Regeln für sichere Passworte zur Anwendung kommen und das Passwort nicht an Unbefugte weitergegeben wird. Zusätzlich muss der USB-Stick vor einer unerlaubten Entfernung geschützt werden. Auch die Sicherungskopie des Schlüssels muss sicher verwahrt werden.

Des Weiteren muss vom Krankenhaus verhindert werden, dass unberechtigte Personen von innerhalb und außerhalb des Krankenhauses Zugriff auf unverschlüsselte Daten des Radiologiesystems oder den Schlüssel erhalten. Dies betrifft sowohl den Anmeldevorgang am System, als auch den physischen wie den Remote Zugriff auf den Server, die z.B. durch starke Authentifizierungsmaßnahmen und räumliche Absicherung verhindert werden müssen.

Zusätzlich muss die Datenübertragung über die externe Anbindung des Radiologiesystems an das Rechenzentrum abgesichert werden. So kann z.B. mittels VPN, Zugangskontrollen und Firewalls zum einen dafür gesorgt werden, dass kein unbefugter externer Verbindungsaufbau zum Rechenzentrum sowie ins Krankenhaus möglich ist. Zum anderen wird der Transport über verschlüsselte Verbindungen möglich.

Unter diesen Voraussetzungen verstößt meiner Ansicht nach die externe Archivierung von Röntgenbilddaten nicht gegen das Bayerische Krankenhausgesetz.

Die dargelegten Wertungen haben auch Auswirkungen auf standes- und strafrechtliche Vorschriften, die das Arztgeheimnis betreffen. Wenn geeignete technische und organisatorische Maßnahmen getroffen werden, kann aus meiner Sicht die Möglichkeit der unbefugten Kenntnisnahme durch einen Dritten praktisch ausgeschlossen werden. Damit würde kein unbefugtes Offenbaren vorliegen, das standes- oder strafrechtlich sanktioniert wäre.

22.2.3.3 JobCard-Verfahren

Angestoßen durch eine Initiative der Bundesregierung, wird derzeit unter der Führung der ITSG (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung) GmbH an Realisierungsmöglichkeiten für das JobCard-Verfahren gearbeitet. Ziel dieses Verfahrens ist es, durch ausschließlich elektronische Datenübermittlung zwischen Arbeitgebern und Leistungserbringern den Aufwand für die Erstellung von arbeitsbezogenen Bescheinigungen deutlich zu reduzieren. Dazu soll zukünftig ein standardisierter Datensatz mit Einkommens- und Beschäftigungsdaten als Basis für die unterschiedlichen Bescheinigungen (z.B. Arbeitsbescheinigung, Verdienstbescheinigungen zur Berechnung von Wohngeld, Kindergeld etc.) regelmäßig vom Arbeitgeber an eine zentrale Speicherstelle (ZSS) übermittelt und dort bei Bedarf durch die Mitarbeiter der Agentur für Arbeit abgerufen werden. Den Zugriff für den Mitarbeiter der Agentur gewährt der betroffene Arbeitnehmer über eine signaturgesetzkonforme Chipkarte, die für das JobCard-Verfahren angemeldet wurde. Durch das JobCard-Verfahren soll eine Entlastung der Arbeitgeber und der Abbau von Bürokratie erreicht werden.

Zur Überprüfung der technischen Machbarkeit wurde in einem ersten Projekt JobCard I, das im April 2004 abgeschlossen wurde, der Abruf der Arbeitsbescheinigung nach § 312 SGB III getestet. Bis 30.06.2005 läuft ein Modellversuch ebenfalls mit virtuellen Personen und mit weiteren 17 Bescheinigungen, deren entsprechende Eignung im Rahmen des Modellversuchs geprüft werden soll. Anschließend soll, nach einer Ausschreibung, die bundesweite Realisierung des Verfahrens beginnen. Geplant ist, das Verfahren zum 01.01.2007 für alle Arbeitnehmer verpflichtend einzuführen.

Da das JobCard-Verfahren komplexe datenschutzrechtliche sowie technisch-organisatorische Fragen aufwirft, wurde auf meine Initiative eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu diesem Thema ins Leben gerufen, die im Mai 2004 das erste Mal zusammentrat und deren Moderator ich bin.

Ich hielt eine intensive Diskussion des JobCard-Verfahrens unter anderem vor dem Hintergrund des Volkszählungsurteils des Bundesverfassungsgerichts für notwendig. Denn aus diesem Urteil kann auch abgeleitet werden, dass es dem Staat untersagt ist, zentrale Datenbestände aufzubauen, für jeden Bürger ein Personenkennzeichen zu vergeben und es Behörden dann zu ermöglichen, beliebige Daten aus diesem zentralen Datenbestand abzurufen. Insbesondere die Schaffung zentraler Datenbestände ist aus Datenschutzsicht immer mit Vorsicht zu betrachten, da diese Begehrlichkeiten wecken und Missbrauchsmöglichkeiten eröffnen. Dabei sollte man sich nicht zu sehr auf rechtliche Sicherungen verlassen, sondern möglichst schon mit technischen Mitteln Gefährdungen für das Recht auf informationelle Selbstbestimmung ausschließen. Bereits von daher bedurfte die Entwicklung des JobCard-Verfahrens einer kritischen Begleitung durch den Datenschutz.

Das JobCard-Verfahren wirft jedoch noch weitere Probleme auf. So ist es ein allgemeiner datenschutzrechtlicher Grundsatz, dass Daten nur erhoben werden dürfen, wenn es für die Aufgabenerfüllung einer Behörde auch erforderlich ist. Dieser Punkt ist im vorgeschlagenen Verfahren problematisch. Denn das JobCard-Verfahren soll für alle Arbeitnehmer verpflichtend eingeführt werden. Somit werden für alle Arbeitnehmer monatlich, unabhängig vom Bedarfsfall, Einkommensdaten an eine zentrale Stelle übertragen. Im Zeitpunkt der Datenerhebung ist noch überhaupt nicht klar, ob eine Behörde überhaupt jemals diese Daten benötigen wird. So ist es zweifelhaft, ob man im Hinblick auf eine zukünftige Kindergeldgewährung bereits Einkommensdaten erheben darf, wenn jemand überhaupt keine Kinder hat. Hier wird das Problem der „Datenspeicherung auf Vorrat“ berührt.

Weiter ist bei der Datenverarbeitung und -nutzung der Grundsatz der Zweckbindung zu beachten. Auch diesbezüglich war das JobCard-Verfahren kritisch zu untersuchen. Schließlich gebietet es die Rechtssicherheit, die Verantwortlichkeiten und den Status der beteiligten Stellen bereits im vorhinein exakt zu definieren. Dies ist unter anderem deshalb erforderlich, damit der Bürger weiß, an welche Stelle er sich im Zweifelsfall wenden kann.

All diese Fragen müssen zunächst mit den Entwicklern des Konzepts kritisch erörtert werden. In einem weiteren Schritt sind dann die wohl erforderlichen Gesetzgebungsarbeiten mit datenschutzrechtlichem Sachverstand zu begleiten.

Geplanter Realisierungsansatz

Die von der ITSG vorgestellte technische Realisierung des JobCard-Verfahrens sieht einen standardisierten Datensatz vor, der Informationen zu Beschäftigungszeiten, Entgeltzahlungen sowie Angaben zur Auflösung von Beschäftigungsverhältnissen enthält. Er wird vom Arbeitgeber regelmäßig in verschlüsselter Form über eine gesicherte Internet-Verbindung an die ZSS übertragen. Dort wird der Datensatz vor der Speicherung temporär entschlüsselt, um Plausibilitätskontrollen durchzuführen und anschließend mit einem Masterkey-Verfahren verschlüsselt und in der Datenbank der ZSS abgelegt. Die Datensätze werden dort so lange aufbewahrt, wie sie für die Bearbeitung durch die Arbeitsagentur benötigt werden, mindestens jedoch sieben Jahre. Besteht auf Seiten des Arbeitnehmers Bedarf an einer arbeitsbezogenen Bescheinigung, z.B. im Falle der Arbeitslosigkeit, wendet er sich an die Agentur für Arbeit. Mit Hilfe seiner JobCard signiert er eine (elektronische) Vollmacht, die dem Mitarbeiter der Arbeitsagentur den Zugriff auf die Daten des Arbeitnehmers erlaubt. Der Mitarbeiter muss sich für den Zugriff über eine Chipkarte authentifizieren. Die Daten des Betroffenen werden bei der ZSS angefragt, dort mit dem Masterkey entschlüsselt, mit dem Schlüssel der Arbeitsagentur neu verschlüsselt und über eine gesicherte Verbindung übertragen. Die Arbeitsagentur kann die Daten für den Zeitraum der Antragsbearbeitung nutzen. Zudem kann der Betroffene zustimmen, dass Daten, die in einem bestimmten Zeitraum nach Antragstellung eintreffen, ebenfalls entschlüsselt und abgerufen werden dürfen, um ein wiederholtes Erscheinen unnötig zu machen.

Zur technischen Absicherung der Datenübertragung und -speicherung werden verschiedene Maßnahmen ergriffen. Sowohl die Arbeitgeber als auch die Arbeitsagentur kommunizieren mit der ZSS über verschlüsselte SSL-Verbindungen. Zusätzlich werden auch die einzelnen Datensätze verschlüsselt. Die Internetanbindung der ZSS ist über Firewalls abgesichert. Dahinter liegen jeweils ein äußeres und inneres Sicherheitssystem, die die Kommunikationspartner verifizieren, die Vollmacht für den Datenzugriff überprüfen, die Daten umschlüsseln und Plausibilitätschecks durchführen. Erst danach erfolgt der Zugriff auf die Datenbank.

Problematik, alternative Ansätze

Eine Kernproblematik bei obigem Realisierungsvorschlag besteht aus technisch-organisatorischer Datenschutzsicht darin, dass die ZSS die technische Möglichkeit hat, sämtliche Daten zu entschlüsseln, da sie im Besitz der verschlüsselten Daten und des Masterkeys ist. Sie kann somit technisch betrachtet alle gespeicherten Daten der Arbeitnehmer ungehindert einsehen ohne selbst die Stelle zu sein, die die Daten für ihre Aufgabenerfüllung benötigt. Daher werden derzeit zwischen der Arbeitsgruppe und der ITSG

GmbH verschiedene andere Lösungsansätze diskutiert.

Ein Ansatz ist die Ende-zu-Ende-Verschlüsselung der Daten jeweils mit dem Schlüssel des Betroffenen. Grob skizziert werden in diesem Fall die Datensätze des Arbeitgebers jeweils mit dem öffentlichen Schlüssel des betroffenen Arbeitnehmers (Verschlüsselungsschlüssel auf der Signaturkarte) verschlüsselt und an die ZSS übermittelt. Dadurch ist nur der Eigentümer der JobCard in der Lage, eine Entschlüsselung vorzunehmen. Identifikationsmerkmal zur Speicherung des verschlüsselten Datensatzes und zum Zugriff ist die UniqueID der Chipkarte des Arbeitnehmers. Eine Nutzung der Daten durch den Sachbearbeiter des betroffenen Amtes ist nach diesem Konzept nur nach Entschlüsselung der Daten mit dem privaten Schüssel des Arbeitnehmers möglich, wodurch dieser die alleinige Kontrolle über seine Daten hat. Anschließend können die Daten auf dem Client des Mitarbeiters im Klartext im Rahmen des Bearbeitungsvorgangs gespeichert werden. Die Umsetzbarkeit eines derartigen Verfahrens soll nach den Vorstellungen der Arbeitsgruppe durch ein Gutachten überprüft werden.

Bisherige Ergebnisse der Arbeitsgruppe

Die Arbeitsgruppe, insbesondere die Vertreter der Landesbeauftragten für den Datenschutz, favorisieren die Ende-zu-Ende-Verschlüsselung gegenüber dem Verfahren der ITSG, aber auch gegenüber den anderen Alternativvorschlägen, die das Problem der technischen Entschlüsselbarkeit des gesamten Datenbestandes häufig nur verlagern, nicht aber beheben. Da jedoch deutlich wurde, dass im laufenden Pilotprojekt JobCard II keine grundsätzlichen konzeptionellen Änderungen mehr möglich sind, wurde in einer Sitzung der Arbeitsgruppe am 09.09.2004 folgendes Vorgehen beschlossen, um im endgültigen Verfahren Verbesserungen des Verfahrens im Hinblick auf den Datenschutz zu erlangen:

- Die Landesdatenschutzbeauftragten sind der Auffassung, dass eine Speicherung personenbezogener Daten des Betroffenen nur zugelassen werden sollte, wenn dieser die technische Verfügungsbefugnis hat (z.B. Ende-zu-Ende-Verschlüsselung mit Schlüssel des Betroffenen).

- Diese sind der Meinung, dass mit einer Ende-zu-Ende-Verschlüsselung der Arbeitnehmerdaten eine Alternative zum bisherigen Ansatz zur Diskussion steht, mit der eine datenschutzgemäße Realisierung des JobCard-Verfahrens möglich erscheint.

- Da deutlich wurde, dass im Hinblick auf den fortgeschrittenen Stand der Pilotprojekte eine Implementierung in das Pilotprojekt JobCard II nicht mehr realisiert werden kann, schlagen die Datenschutzbeauftragten vor, parallel zur Abwicklung des Projekts JobCard II eine Untersuchung über die Integrierbarkeit der Ende zu Ende Verschlüsselung in das JobCard-Verfahren in Auftrag zu geben, deren Ergebnisse in der endgültigen Ausschreibung des JobCard-Verfahrens berücksichtigt werden sollen.

Die Datenschutzkonferenz hat am 29.10.2004 den Vorschlag der Arbeitsgruppe aufgegriffen und zustimmend zur Kenntnis genommen. Sie hat den Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder beauftragt, die näheren Rahmenbedingungen für den Gutachtenauftrag zu definieren. Gleichzeitig hat sie den Bundesbeauftragten gebeten, das BMWA auf dieser Grundlage um Vergabe eines Gutachtens an einen neutralen Gutachter zur Realisierbarkeit der Ende-zu-Ende-Verschlüsselung zu bitten.

22.2.3.4 Telematikplattform für medizinische Forschungsnetze (TMF), Kompetenznetze

Im Berichtszeitraum war ich auch mit der Bewertung der technisch-organisatorischen Datenschutzkonzepte verschiedener medizinischer Kompetenznetze befasst. Die Kompetenznetze dienen dem Aufbau von Vernetzungsstrukturen zur Durchführung bundesweiter klinischer Studien bezüglich einzelner chronischer und schwerer Erkrankungen über längere Zeiträume hinweg an großen Patientengruppen. Eine Übersicht hierzu bietet www.kompetenznetze-medizin.de/. Derartige Kompetenznetze werfen meist ähnliche datenschutzrechtliche und technische Schwierigkeiten bei der Realisierung auf:

- Wissenschaftliche Langzeitbeobachtung chronisch kranker Patienten

- Nutzung von Patientendaten im Forschungs- und Behandlungszusammenhang

- Dokumentation durch mehrere behandelnde Stellen

Um diesen Anforderungen zu begegnen, wurde von der Telematikplattform für medizinische Forschungsnetze (TMF) e.V. (www.tmf-net.de) ein generisches Datenschutzkonzept entwickelt. Die TMF e.V., in deren Beirat ich Mitglied bin, ist ein Zusammenschluss medizinischer Forschungsverbünde zur För-

derung vernetzter Strukturen, mit dem Ziel, geeignete IT-Infrastrukturen zu schaffen.

Das generische Datenschutzkonzept wurde von der TMF in enger Abstimmung mit dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder entwickelt, um die bundesweite Verwendbarkeit zu gewährleisten. Es wurde im März 2003 vom AK Wissenschaft angenommen und steht seitdem als Basis für die Realisierung der einzelnen Kompetenznetze zur Verfügung.

Neben den Regeln zur Erfassung und Speicherung medizinischer Patientendaten berücksichtigt das Konzept auch die organisatorische und logistische Einbeziehung von Laborproben und Biomaterialien. Insbesondere enthält es Vorgehensweisen zur Qualitätssicherung bei der Datenerfassung und die Bedingungen zur nachträglichen Reidentifikation von Patienten, um sie über wichtige wissenschaftliche Erkenntnisse informieren zu können. Um den verschiedenen Arten von Studien gerecht zu werden, wurden zwei Lösungsvarianten erarbeitet: klinisch fokussierte Forschungsnetze und wissenschaftlich fokussierte Forschungsnetze.

Klinisch fokussierte Forschungsnetze

In diesem Fall werden die Daten direkt aus dem klinischen Behandlungsprozess heraus erhoben, da die Forschungsergebnisse dem Behandler direkt zur Verfügung stehen sollen. Gleichzeitig dürfen für wissenschaftliche Auswertungen jedoch keine identifizierenden Daten der Patienten genutzt werden. Daher wurde eine getrennte Datenhaltung eingeführt: Die identifizierenden Daten (Name, Adresse etc.) werden zusammen mit einer daraus generierten, eindeutigen PID (Patientenidentifikator) in einer Patientenliste abgespeichert. Die Behandlungsdaten werden nur mit dieser PID, ohne die identifizierenden Daten, in der Behandlungsdatenbank abgelegt. Der behandelnde Arzt kann bei Bedarf temporär Daten der beiden Bestände online zusammenführen (nach entsprechender Berechtigungsprüfung), für den wissenschaftlichen Zugriff erfolgt ein Export von Daten ohne PID, sodass kein Online-Zugriff auf die Behandlungsdaten besteht.

Wissenschaftlich fokussierte Forschungsnetze

In diesem Fall erfolgt die Erfassung der Daten getrennt vom Behandlungsprozess. Die Schwierigkeit besteht dabei darin, die Qualität der erfassten Daten sowie eine Fortschreibung der Daten bei chronischen Erkrankungen sicherzustellen, ohne dem Wissenschaftler Zugang zu identifizierenden Patientendaten zu ermöglichen. Die identifizierenden Daten werden daher wiederum mit einer PID versehen und in einer separaten Patientenliste gespeichert. Den medizinischen Daten wird ebenfalls die PID zugeordnet und sie werden im ersten Schritt an die Qualitätskontrolle weitergegeben, die eine Nacherfassung veranlassen kann. Danach werden die Daten mit einem von der TMF definierten Verfahren pseudonymisiert, d.h. die PID wird mittels kryptografischer Transformation durch ein Pseudonym (PSN) ersetzt, und in der Forschungsdatenbank abgelegt, auf die die Wissenschaftler online zugreifen können. Die Rückführung des PSN ist für die Wissenschaftlicher technisch nicht möglich, hierzu muss ein definiertes Verfahren mit mehreren Beteiligten angestoßen werden.

Technische Sicherheitsmaßnahmen

Beide Teilkonzepte enthalten gewisse obligatorische Basissicherheitsmechanismen. Dies beinhaltet die Verschlüsselung sämtlicher Datenübertragungen via SSL, also sowohl bei der Erfassung der Daten, die meist über ein Web-Formular erfolgt, als auch beim Transport der Daten zwischen verschiedenen Datenbanken. Da die Übermittlung teilweise über das Internet erfolgt, müssen die beteiligten Geräte gegen Angriffe und Schadenssoftware geschützt werden (Firewall, Virenscanner etc.). Die Absicherung der beteiligten Rechenzentren wird als gegeben angenommen. Eine weitere Maßnahme ist die verschlüsselte Datenspeicherung der identifizierenden Daten in der Patientenliste einerseits und der medizinischen Daten in den Forschungs-/Behandlungsdatenbanken andererseits.

Auch Basisrichtlinien zur Vergabe von Zugriffsberechtigungen wurden definiert. So haben z.B. im klinisch fokussierten Ansatz nur die behandelnden Ärzte Online-Zugriff auf die Daten ihrer Patienten. Als Basis der Zugriffsrechte auf der Behandlungsdatenbank wird die Zuordnung Arzt – Patient in der Patientenliste abgespeichert. Über ein Rollenkonzept können einzelnen Personen mit verschiedenen Aufgaben jeweils angemessene Rechte zugeteilt werden. Löschbefugnisse für die Patientendaten sind für Ärzte grundsätzlich ausgeschlossen. Um eine Kenntnisnahme der Gesamtdaten bzw. ihre Zusammenführbarkeit durch einen Administrator zu verhindern, werden Patientenliste und Behandlungsdatenbank getrennt administriert und häufig an verschiedenen Stellen gespeichert. Zudem dürfen die Administratoren nicht an der Behandlung oder wissenschaftlichen Verwertung beteiligt sein. Zur Gewährleistung der Revisionssicherheit werden alle datenschutzrelevanten Vorgänge protokolliert.

In wissenschaftlich fokussierten Forschungsnetzen spielt die Sicherheit des Schlüssels zur Pseudonymgenerierung eine große Rolle, da ansonsten die PID ermittelt werden kann. Deshalb wird der Schlüssel auf passwortgeschützten SmartCards gespeichert, die sicher verwahrt werden müssen. Für die Pseudonymi-

sierung, und somit für die Aufnahme der Daten in die Forschungsdatenbank, authentifizieren sich die Beteiligten wechselseitig über SSL und es werden nur Daten von zugelassenen Sendern entgegen genommen. Die medizinischen Daten selbst liegen während der Pseudonymisierung nur verschlüsselt vor, da sie von der Qualitätssicherung ver- und erst in der Forschungsdatenbank wieder entschlüsselt werden. Die hierzu benötigten Schlüssel sind ebenfalls auf einer SmartCard gespeichert.

Beispiele für Kompetenznetze

Trotz der generischen Datenschutzkonzepte unterscheiden sich die verschiedenen Kompetenznetze im Detail voneinander, sodass jeweils eine genauere Ausgestaltung des gewählten Basiskonzepts nötig ist. In deren Bewertung sind auch jeweils die Landesbeauftragten für Datenschutz eingebunden. Die aktuellsten Beispiele sind die Kompetenznetze Herzinsuffizienz und HIV/ AIDS.

Das Kompetenznetz Herzinsuffizienz, das federführend vom Berliner Beauftragten für Datenschutz und Informationsfreiheit betreut wird, umfasst eine größere Anzahl von Teilprojekten zu diesem Krankheitsbild. Das Datenschutzkonzept orientiert sich an dem für wissenschaftlich orientierte Forschungsnetze. Dabei wurde allerdings für die benötigte verteilte Datenhaltung die Systemstruktur (normalerweise bestehend aus Patientenliste und Forschungsdatenbank) deutlich erweitert und enthält darüber hinaus Studien- und Projektdatenbanken. Zudem musste dem Umstand Rechnung getragen werden, dass ein Patient Teilnehmer mehrerer Studien sein kann, ohne eine Verschlechterung des Datenschutzes zu bewirken. Beides macht die Festlegung weiterer angemessener technischer Sicherheitsmaßnahmen erforderlich.

Auch das Kompetenznetz HIV/AIDS (Federführung Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen) orientiert sich am Datenschutzkonzept für wissenschaftlich fokussierte Forschungsnetze. Änderungsbedarf zum generischen Konzept bestand hier bezüglich des Monitorings und der Replikation der Forschungsdatenbank. Der Monitor überprüft stichprobenartig Fälle aus der Datenbank mit den Originaldaten vor Ort, wodurch er Einblick in patientenbezogene medizinische Daten erhält, der geregelt werden muss. Insbesondere durch die Replikation der Datenbanken zu Zwecken der Qualitätssicherung wird die technische Infrastruktur über das Basiskonzept hinaus erweitert, sodass hier entsprechende Sicherheitsmechanismen definiert werden müssen.

22.2.3.5 Portal-Technologie

Im Berichtszeitraum wurde ich mit dem Projekt „GeoPortal“ aus der High Tech-Offensive (HTO) der Bayerischen Staatsregierung befasst. Im Mittelpunkt von GeoPortal steht die Überprüfung der Realisierbarkeit eines Einstiegsknotens im Internet, über den mehrere bei unterschiedlichen speichernden Stellen vorgehaltene Datenbanken miteinander verknüpft werden können. Einem autorisierten Benutzer sollen die Ergebnisdaten für seine Abfrage ungeachtet des physikalischen Speicherortes „in einem Zuge“ präsentiert werden; der Benutzer braucht keinerlei Kenntnis über die Verfügbarkeit oder tatsächlichen Speicherorte der angefragten Daten zu haben – er bedient sich lediglich eines „Web-Services“.

Für das Projekt wurden

- staatliche Daten (die Digitale Flurkarte (DFK) eines staatlichen Vermessungsamtes, digitale Orthofotos, die Digitale Topographische Karte 1:25.000 und Georeferenzierte Adressen des Bayerischen Landesvermessungsamtes sowie Daten des Raumordnungskatasters (ROK) des Ministeriums für Landesentwicklung und Umweltfragen), die sich innerhalb des Bayerischen Behördennetzes befinden,

- gemeindliche Daten (Automatisiertes Liegenschaftsbuch (ALB)), die sich innerhalb des gemeindlichen Intranets befinden, und

- externe Daten (z.B. Bebauungspläne), die sich im Internet verteilt befinden, durch die Technische Universität München simuliert und

für autorisierte Mitarbeiter einer Pilotgemeinde virtuell miteinander kombiniert.

Die technische Machbarkeit konnte im Pilotprojekt gezeigt werden. Die Einbindung weiterer Datenbestände ist denkbar. Durch diese virtuelle Zusammenführung und Aggregierung der über mehrere Netzwerke verteilten Daten könnten für die öffentliche Verwaltung und auch für den Bürger z.B. im gesamten Bereich der Baugenehmigungsverfahren erheblicher Aktualitäts- und Komfortgewinn sowie erhebliches Einsparpotenzial realisiert werden.

Ganz entscheidend für die Zulässigkeit derartiger Systeme sind aber die Einhaltung gesetzlicher Normen betreffend

- die Zweckbindung der jeweiligen Datenbestände,

- die Zulässigkeit eines (automatisierten) Datenabrufs,

- die durchgängige Sicherstellung von Authentizität, Integrität und Vertraulichkeit der Daten sowie

- eine zuverlässige Benutzerverwaltung mit Zugriffskontrolle und jeweiliger Netzabsicherung.

Wichtiges Werkzeug in diesem Zusammenhang ist wieder einmal die Kryptographie in Form von elektronischer Signatur, Zertifikaten und Nutzdatenverschlüsselung. Auch ohne funktionierende Public Key Infrastruktur (PKI) wird etwas Derartiges für eine Praxisanwendung nicht zu realisieren sein. Ich konnte hier meine Anregungen einbringen.

Wenngleich auch noch einige Detailfragen in diesem Projekt offen blieben, so erscheint es doch wegweisend für evtl. weitere Vorhaben auch aus anderen Bereichen. Es hat jedenfalls deutlich gezeigt, dass gerade bei derart komplexen Systemen eine frühzeitige Einbindung meiner Dienststelle unabdingbar ist und nur so Fehlentwicklungen oder gar unzulässige Entwicklungen vermieden werden können.

22.3 Technische Einzelprobleme

22.3.1 USB Memory Sticks

USB steht für "Universal Serial Bus" und wurde 1995 als Industrie-Standard entwickelt, um periphere Geräte an Computer anzuschließen und alte Schnittstellen, wie parallele, serielle oder PS/2 zu ersetzen. In der aktuellen Version 2.0 unterstützt USB Übertragungsraten von bis zu 480 Mbit/s und es können bis zu 127 unterschiedliche Geräte an einen Bus angeschlossen werden.

Nahezu jeder heute aktuelle PC wird mit einer USB Schnittstelle ausgeliefert. Die neuesten Modelle verwenden deswegen zum Teil keine der alten Schnittstellen mehr, sodass Tastatur, Maus und Drucker nur noch über USB angeschlossen werden können. Ein Arbeiten ohne USB ist an solchen Workstations somit nicht mehr möglich.

Sobald ein PC eine USB-Schnittstelle hat, kann an diese die oben genannte große Anzahl an Geräten angeschlossen werden. Auch wenn alle USB-Steckplätze am Gehäuse z.B. durch Maus und Tastatur bereits belegt sind, lässt sich problemlos ein USB-Hub dazwischen stecken, der dann zusätzliche freie Schnittstellen bietet.

Betrachtet man die Geräteklassen, die für USB erhältlich sind, so ist dies die gesamte Palette an Hardware, angefangen von Druckern, Kameras, Kartenleser und Massenspeicher (USB Memory Sticks) bis hin zu Modems, Netzwerk- und WLAN-Karten.

Bisher reichte es aus, bei einem PC die Disketten und CD-ROM Laufwerke zu sperren, um unberechtigten Datenaustausch über Speichermedien zu unterbinden. Mit USB Memory Sticks stehen sehr kleine (Schlüsselanhänger) und sehr große (über ein Gbyte Speicher) Speichermedien bereit, die sogar im laufenden Betrieb angesteckt und wieder entfernt werden können.

Hieraus ergeben sich folgende Risiken:

- Aktuelle BIOS Versionen unterstützen das Booten von USB Medien. Somit lassen sich die Schutzmechanismen des auf den PC installierten Betriebssystems leicht umgehen, wenn von einem Betriebssystem über USB gebootet wird, das unter der Kontrolle des Angreifers steht.

- Durch im laufenden Betrieb angesteckte USB Memory Sticks kann Schadsoftware eventuell unkontrolliert eingeführt werden, denn nicht alle Virenscanner prüfen auch USB Geräte automatisch.

- Durch die hohe Speicherkapazität und die hohe Geschwindigkeit ist es sehr einfach, eine große Menge eventuell sensibler oder personenbezogener Daten unberechtigt und unkontrollierbar außer Hause zu bringen.

- Auch das Anschließen von Netzwerkkarten, Bluetooth-Adaptern, Modems und WLAN-Karten über USB bietet einen einfachen Weg, vorhandene Firewalls und andere Restriktionen zu umgehen und unkontrollierte Verbindungen aufzubauen.

- Aufwändige Installationsprozeduren für Hard- und Software entfallen, da moderne Betriebssysteme die neu angeschlossenen Geräte sofort einbinden. Dadurch sinkt die Hemmschwelle, nicht freigegebene, mitunter sogar auch private Technik zu nutzen.

- Die bisher eingerichteten Nutzungsbeschränkungen für CD- und Floppy-Laufwerke sind deshalb nicht mehr ausreichend wirksam. Es müssen folglich Mechanismen gefunden werden, mit denen der Zugriff auf den USB auf genau die zugelassenen Geräte beschränkt werden kann.

Ein Überblick über die Möglichkeiten zur sicheren USB Konfiguration unter Windows und Linux findet sich in der Orientierungshilfe „Datensicherheit bei USB-Geräten“, die von meiner Home-Page unter www.datenschutz-bayern.de/technik/orient/usb.html abgerufen werden kann.

22.3.2 RFID-Technologie

RFID steht für Radio Frequency Identification und ist eine Technologie, die durch Funkwellen eine kontaktlose automatische Identifikation von Gegenständen ermöglicht, die mit einem RFID-Etikett versehen sind.

Die Bauformen der RFID-Etiketten können verschiedenen Einsatzzwecken angepasst werden. Aufgrund ihrer geringen Größe können sie beispielsweise in Verpackungen, Chipkarten und vielen anderen Produkten und Alltagsgegenständen integriert werden. Hauptanwendungsgebiete sind zurzeit die Bereiche Industrieautomation, Zutrittssysteme, Tieridentifikation, Warenmanagement und elektronische Wegfahrsperren.

Warum bringen RFID-Etiketten Gefahren für den Datenschutz?

Ein RFID-Etikett an sich ist aus Datenschutzsicht nicht gefährlich. Solange es nicht in die Nähe eines Lesegerätes kommt, ist es vollkommen inaktiv. Besitzt ein Produkt ein RFID-Etikett und passiert es ein Lesegerät, so werden die Daten, die auf dem Etikett gespeichert sind, ausgelesen. Die Datenmenge auf einem RFID-Etikett kann von einem Bit bis hin zu mehreren Kilobytes gehen. Es gibt des Weiteren auch RFID-Etiketten, die einen kompletten Rechner beinhalten, sodass Lese-, Schreib- und Rechenoperationen bis hin zu kryptografischen Verfahren möglich sind. Diese intelligenten RFID-Etiketten sind zurzeit zwar noch sehr teuer, aber werden wie alle Neuerungen in der IT vermutlich sehr bald sehr billig werden.

Ein RFID-Etikett ist grundsätzlich anders zu würdigen als z.B. die bisher übliche einfache Produktgruppennummer in Form eines Barcodes. Ein Barcode wird etwa an einer Supermarktkasse mit Hilfe eines Barcode Scanners ausgelesen. Bei einem Barcode ist die Datenerhebung (also das Einlesen durch die Kassiererin) offen und für den Kunden erkennbar. Auch bei einem RFID System wird der Kunde davon ausgehen, dass an der Kasse ein Lesegerät steht. Da das Auslesen aber nicht mittels eines räumlich sehr begrenzten und exakt positionierten Gerätes funktioniert, sondern mit Funkwellen, kann der Kunde nicht feststellen, wo genau RFID-Etiketten ausgelesen werden. Schon das Regal kann, wenn es entsprechend ausgestattet ist, feststellen, welche Produkte entnommen werden. Natürlich ist dies aufwändig und wird nicht im ersten Schritt passieren. Zuerst werden die RFID-Etiketten zur Transportkontrolle und zur Lagerverwaltung usw. verwendet werden. Aber wenn dann alle Produkte damit ausgestattet sind und sich die Systeme in „einfachen“ Umgebungen bewährt haben, wird man sie immer mehr einsetzen.

RFID-Etiketten sind ohne Berührung auslesbar. Betritt der Kunde ein Geschäft und führt bereits Waren mit RFID-Etiketten aus anderen Geschäften mit sich, so lassen sich auch deren RFID Informationen auslesen. Das heißt, jedes Geschäft kann in den Inhalt der Einkaufstaschen seiner Kunden sehen und diesen theoretisch auch automatisch speichern. Die Haltbarkeit von RFID-Etiketten ist zeitlich nicht begrenzt, selbst nach Jahren dürften sie lesbar sein, da sie keine eigene Energieversorgung etwa in Form von Batterien benötigen.

Noch deutlicher wird die potenzielle Gefahr für den Datenschutz, wenn man einmal nicht vom normalen Haushaltseinkauf ausgeht, sondern beispielsweise an gekaufte Medikamente denkt. An jedem Punkt im Umkreis von bis zu 20 Metern kann, wenn es mit RFID-Etiketten versehen ist, jedes Medikament in der Tasche eines Bürgers unbemerkt von jedem Lesegerät gelesen werden.

Werden, wie von der Europäischen Zentralbank im Moment für die größeren Geldscheine geplant, irgendwann einmal auch alle Geldscheine mit RFID-Etiketten versehen sein, so kann jeder auch feststellen, wie viel Geld dieser Bürger bei sich führt, inklusive der Nummern aller Geldscheine.

Solange nur Produkte mit RFID-Etiketten ausgestattet werden, kann man argumentieren, dass ein direkter Personenbezug schwierig bzw. in der Regel nicht vorhanden ist. Das Lesegerät erkennt nur, dass Medikament X an ihm vorbeigetragen wurde, nicht aber, wer dieses Medikament besitzt. Betrachtet man aber die Bestrebungen, auch Kreditkarten und Ausweispapiere mit RFID- Etiketten auszustatten, so ist ein Personenbezug nicht nur machbar, sondern oft nicht mehr zu verhindern. Eventuell protokolliert ein Lesegerät alle Daten der RFID-Etiketten, die an ihm vorbeikommen. Die Ausweisnummer, den Namen und die Anschrift aus dem RFID-Etikett des Personalausweises, alle Bankverbindungsdaten und Kreditkartennummern sowie alle Produkte und alles Bargeld, das eine Person bei sich führt. Und das eventuell völlig unbemerkt vom Eigentümer dieser Informationen und ohne dass er es einfach verhindern kann.

Nicht betrachtet in den bisherigen Beispielen sind mit einer Vielzahl von Lesegeräten verknüpfte, zentrale Datenbanken, die alle erfassten Daten sammeln,

so dass damit für Personen sehr genaue Bewegungs- und Verhaltensprofile gespeichert werden könnten, deren Qualität weit über die potenziellen Bewegungsprofile etwa durch ein Mobiltelefon (das nur vom Netzbetreiber alleine protokolliert und im Vergleich zum RFID-Etikett vom Besitzer ausgeschaltet werden kann) hinausgehen.

Deshalb heben die Internationale Konferenz der Datenschutzbeauftragten und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihren Entschließungen die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen (s. Anlage 17). Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID Systemen berücksichtigt werden. Insbesondere

- soll jeder vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

- wenn personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

- dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zur Erreichung dieses Zwecks erforderlich ist und

- so weit RFID-Etiketten im Besitz von Personen sind, sollen diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

22.3.3 Trusted Computing

Der Begriff „Trusted Computing“ soll hier als allgemeiner Oberbegriff verwendet werden für die Initiative von mehr als 130 Firmen, darunter die Firmen Microsoft, Intel, IBM, HP, AMD, Sony Corporation und Sun Microsystems, den PC-Einsatz vertrauenswürdiger zu machen. Trusted Computing (TC) war die erste Bezeichnung hierfür. In den Diskussionen taucht weiterhin die „Trusted Computer Platform Alliance“ (TCPA) auf, die dann zur „Trusted Computing Group“ (TCG) umbenannt wurde - einer Firma, die unter anderen von den oben genannten Unternehmen gegründet wurde. Die geplante Softwareumsetzung von TC in Windows Betriebssystemen wurde als „Palladium“ bzw. mit neuem Namen „Next Generation Secure Computing Base“ (NGSCB) für die geplante nächste Version („Longhorn“) angekündigt.

Trusted Computing Modul

In einem mit TC geschützten PC gibt es ein „Trusted Computing Modul“ (TCM), dessen Funktionen das Vertrauen in die Sicherheit des PC stärken sollen. Unter anderem existieren Funktionen zur Verwaltung kryptografischer Schlüssel, zum sicheren Booten eines PC, zur Authentisierung, zur Protokollierung, zur Initialisierung und für weitere Managementaufgaben. Das TCM stellt dabei eine ausschließlich passive Komponente dar, die das Betriebssystem des PC unterstützt. Für die Nutzung dieser Funktionen sind ein spezielles BIOS und ein angepasstes Betriebssystem nötig. In einigen bereits verfügbaren Hardwarekonfigurationen wird das TCM in Form eines „Fritz-Chips“ als eigener Chip auf dem Motherboard installiert, der unter anderem die privaten Schlüssel des Anwenders analog einer Signaturchipkarte vor der ungewollten Veröffentlichung schützen können soll. Bis jetzt nutzt kein zur Zeit verfügbares Betriebssystem den Fritz-Chip.

Funktionen

Mit Hilfe des TCM und einer entsprechenden Softwarekomponente („Security Support Component“ - SSC) im Betriebssystem sollen im Wesentlichen folgende Funktionen ermöglicht werden:

- Daten können so verschlüsselt werden, dass sie nur mit der aktuellen (sicheren) Systemkonfiguration gelesen werden können, d.h. z.B. nach einer Installation einer neuen (nicht zertifizierten) Betriebssystemkomponente kann auf die Daten nicht mehr zugegriffen werden.

- Es gibt einen durch die Hardware geschützten Speicherbereich, in dem z.B. kryptografische Schlüssel sicher gespeichert werden können. Auf diese kann dann nur mit zertifizierter Soft- und Hardware zugegriffen werden.

- Das System kann sich anderen Systemen als „vertrauenswürdig“ beweisen. Beispielsweise kann ein Anzeigeprogramm für Filme damit dem digitalen Filmverleiher online sicherstellen, dass keine Zusatzkomponenten zur Umgehung des Copyrights auf den ausgeliehenen Film zugreifen können.

- Ein spezieller Zufallsgenerator zur Erzeugung sicherer kryptografischer Schlüssel ist vorhanden.

- Das TCM stellt eine manipulationssichere Echtzeituhr zur Verfügung, sodass sich Zeitstempel sicher prüfen lassen.

Externe Sicherheitsinstanzen

Mit Hilfe von TC lassen sich Transaktionen implementieren und etablieren, die Sicherheitsrichtlinien auch außerhalb des eigenen Einflussbereichs wirksam durchsetzen. Es ist denkbar, dass der Verfasser (Rechteinhaber) eines Dokuments festlegt, auf welchen fremden PCs dieses Dokument verarbeitet werden kann. Das heißt aber, dass das Lesen dieses Dokuments dann davon abhängt, ob die (aus der Sicht des Lesenden externe) Sicherheitsinstanz des Verfassers aktuell erreichbar ist, da der Verfasser auch die Möglichkeit hat, die früher einmal gewährten Rechte zu widerrufen. Auch Software kann so geschützt sein, dass sich eine Softwarekomponente nur dann starten lässt, wenn der PC im TC Modus läuft und der Softwarehersteller das Starten der Software auf diesem PC erlaubt und nicht zwischenzeitlich widerrufen hat.

TC und Datenschutz

Jede dieser Funktionen kann einen PC sicherer machen und damit aktiv zur Verbesserung des Datenschutzes und der Datensicherheit beitragen. Die Datenschutzbeauftragten des Bundes und der Länder begrüßen in der Entschließung „TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden“ der 65. Datenschutzkonferenz alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen (siehe Anlage 2).

Die Datenschutzbeauftragten halten es jedoch für unvertretbar, falls

- Anwenderinnen und Anwender nicht die alleinige Kontrolle über die Funktionen des eigenen Computers behalten,

- die Verfügbarkeit von TC-konformen Arbeitsplätzen und der darauf verarbeiteten Daten dadurch gefährdet wäre, dass zentrale, extern betriebene Sicherheitsinstanzen nicht verfügbar wären,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet (z.B. E-Mail) durch TC-Restriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben einer externen Kontrollinstanz zulässig sein würde und somit eine sehr weit gehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten Gewähr leistet werden.

22.3.4 Automatischer Software-Update (Windows XP)

Für alle zurzeit auf dem Markt befindlichen Betriebssysteme werden von den Herstellern oder Distributoren bei Bedarf Aktualisierungen angeboten, die beispielsweise Sicherheitsprobleme beheben oder neue Funktionalitäten anbieten. Aus der Sicht der Datensicherheit ist die zeitnahe Behebung von Sicherheitsproblemen unabdingbar.

Für derartige Aktualisierungen („Updates“) gibt es grundsätzlich drei Varianten:

- Die Updates werden vom Hersteller zur Verfügung gestellt und der Administrator muss sich darüber informieren, welche Updates für ihn relevant sind.

- Das Betriebssystem benachrichtigt den Anwender/Administrator über neue Updates und fragt, ob diese installiert werden sollen.

- Das Betriebssystem sucht automatisch nach Updates und installiert diese ohne Zustimmung des Anwenders oder Administrators (automatisches Software-Update).

Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen stellen jedoch Wartungstätigkeiten im datenschutzrechtlichen Sinn dar. Deshalb muss sichergestellt sein, dass nur den dazu ausdrücklich ermächtigten Personen die Installation derartiger Updates möglich sein darf. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige automatische Software-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Immer mehr Behörden setzten Windows XP ein oder planen darauf umzusteigen, weil zum Beispiel die bisher eingesetzte Version Windows NT4 nicht mehr vom Hersteller weitergepflegt wird. Windows XP bietet aber als Neuerung ein automatisches Software-Update an. Es ist hier anzuraten, das automatische Update abzuschalten (unter Systemeigenschaften / Automatische Updates) und nur nach vorherigen erfolgreichen Tests die Aktualisierungen einzuspielen. Bei einer größeren Anzahl von Rechnern empfiehlt es sich, alle Updates zentral zu verwalten (etwa über den von Microsoft erhältlichen Windows Update Services WUS) und auch hier Updates nur dann freizugeben, nachdem sie erfolgreich getestet worden sind.

22.4 Orientierungshilfen

Im Berichtszeitraum hat meine Geschäftsstelle alle Orientierungshilfen überarbeitet und auf einen aktuellen Stand gebracht. Neu erstellt wurden die Orientierungshilfen „Einsatz von Funktastaturen“ und „Datensicherheit bei USB-Geräten“. Vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurden die Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ und von einer Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Handreichung „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ erstellt.

Alle Dokumente können von meiner Home-Page unter www.datenschutz-bayern.de abgerufen werden.

23 Die Datenschutzkommission

Der Datenschutzkommission beim Bayerischen 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 G. 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

ab dem 27.11.2003:

Prof. Dr. Hans G. Stockinger	CSU	Christian Meißner	CSU
Petra Guttenberger	CSU	Robert Kiesel	CSU
Joachim Haedke	CSU	Herbert Ettengruber	CSU
Ernst Weidenbusch	CSU	Peter Winter	CSU
Martin Neumeyer	CSU	Peter Schmid	CSU
Bärbel Narnhammer	SPD	Florian Ritter	SPD
Christine Stahl	BÜNDNIS90/ DIE GRÜNEN	Christine Kamm	BÜNDNIS90/ DIE GRÜNEN

Für die **Staatsregierung**:

Christian Peter Wilde	Ministerialrat im Bayerischen Staatsministerium des Innern	Hubert Kranz	Ministerialrat im Bayerischen Staatsministerium der Finanzen

ab dem 27.11.2003:

Hubert Kranz	Ministerialrat im Bayerischen Staatsministerium der Finanzen	Christian Peter Wilde	Ministerialrat im Bayerischen Staatsministerium des Innern

Für die **Sozialversicherungsträger**:

Werner Krempl	Erster Direktor und Geschäftsführer der LVA Oberfranken und Mittelfranken	Dr. Helmut Platzer	Vorstandsvorsitzender der AOK Bayern

ab dem 27.11.2003:

Werner Krempl	Erster Direktor und Geschäftsführer der LVA Oberfranken und Mittelfranken	Dr. Helmut Platzer	Vorstandsvorsitzender der AOK Bayern

Für die **Kommunalen Spitzenverbände**:

Klaus Eichhorn	Geschäftsführender Direktor der AKDB	Wolfgang Kellner	Abteilungsleiter bei der AKDB

ab dem 27.11.2003:

Klaus Eichhorn	Geschäftsführender Direktor der AKDB	Wolfgang Kellner	Abteilungsleiter bei der AKDB

ab dem 30.09.2004:

Wolfgang Kellner	Abteilungsleiter bei der AKDB	Klaus Laumer	Abteilungsleiter bei der AKDB

Für den **Verband freier Berufe e.V.**:

Margit Bertinger	Steuerberaterin und Wirtschaftsprüferin Präsidiumsmitglied des Verbandes Freier Berufe in Bayern	Klaus von Gaffron	Bildender Künstler Präsidiumsmitglied des Verbandes Freier Berufe in Bayern Vorsitzender des BBK München und Oberbayern e. V. Berufsverband Bildender Künstler e.V.

ab dem 27.11.2003:

Hans-Ulrich Sorge	Geschäftsführer des Bayerischen Notarvereins e.V.	Klaus von Gaffron	Präsidiumsmitglied des Verbandes Freier Berufe in Bayern und Berufsverbandes Bildender Künstler Bayern

Den Vorsitz in der Datenschutzkommission führte bis zum Ende der 14. Wahlperiode Franz Brosch, MdL, seine Stellvertreterin war Frau Bärbel Narnhammer, MdL. Seit dem 09.03.2004 führt Professor Dr. Gerhard Stockinger, MdL, den Vorsitz. Stellvertretende Vorsitzende ist weiterhin Frau Bärbel Narnhammer, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im vergangenen Berichtszeitraum sieben Mal. Dabei befasste sie sich insbesondere mit folgenden Themen:

- Vorberatung des 20. Tätigkeitsberichts
- Berichte von Datenschutzkonferenzen
- Neues Melderecht im Internetzeitalter
- Abfrage sensitiver Daten in einem BRK-Altenheim
- ELSTERLohn und eTIN
- Aktuelle Situation der Video-Überwachung in Bayern
- Novellierung des Bayerischen Polizeiaufgabengesetzes

Anlage 1: **Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003**
Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

1. Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

   - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

   - Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.

   - Die Freiwilligkeit der Einwilligung muss gewährleistet sein.

   - Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

2. Technischer Datenschutz

   Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

3. Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

   Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

   Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

4. Förderung von datenschutzgerechter Technik

   Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen

Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

5. Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z.B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

6. Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen - wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung - für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten

werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z.B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts - und zwar nicht nur im Bereich der Telefonüberwachung - als grundrechtssicherndes Verfahrenselement ergreifen muss.

7. Stärkung des Schutzes von Gesundheitsdaten

Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z.B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z.B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

8. Datenschutz und Gentechnik

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26.10.2001 Vorschläge vorgelegt.

9. Datenschutz im Steuerrecht

Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und –speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

10. Arbeitnehmerdatenschutz

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

11. Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

12. Stellung des Bundesdatenschutzbeauftragten

Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

13. Verbesserung der Informationsrechte

Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

Anlage 2: **Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003**
TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz "Trusted Computing Platform Alliance" (**TCPA**).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin mög-

lich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

Anlage 3: **Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003**
Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11.11.2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)" entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. (Die Schutzprofile mit dem Titel „BISS –Benutzerbestimmbare Informationsflusskontrolle" haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter www.bfd.bund.de/technik/protection_profile.html abrufbar.)

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. (Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter www.datenschutzzentrum.de/guetesiegel veröffentlicht.)

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und –Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

Anlage 4: **Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003**
Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patien-

tinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u.a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1.

Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z.B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2.

Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grds. selbst zu entscheiden,

- ob sie überhaupt verwendet wird,
- welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
- welche Daten zu löschen sind und wann das zu geschehen hat,
- ob sie im Einzelfall vorgelegt wird und

- welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin

- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 03.05.2002, wonach "der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3.

Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4.

Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

Anlage 5: **Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003**
Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10 Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

Anlage 6: **Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003**
Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem

Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.01.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen„ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.

  Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,

- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

- eGovernment- und eCommerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,

- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,

- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

Anlage 7: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.03.2003
Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Abs. 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

Anlage 8: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28.04.2003
Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz vom 28.03.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z.B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z.B. PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.03.2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z.B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vor-

rat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z.B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammen.

Anlage 9: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 30.04.2003
Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind . Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.

- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.

- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

Anlage 10: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.07.2003
Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sogen. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr - wie vom geltenden Recht gefordert - in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht-codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z.B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

Anlage 11: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 07.08.2003 zum automatischen Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei - oftmals vom Nutzer unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit prakti-

zierten Umfang aus technischen Gründen erforderlich ist.

- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.

- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das - unbemerkte - Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogen Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

Anlage 12: Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.09.2003 zum Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.

- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z.B. mit data-warehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass

- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

Anlage 13: Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.09.2003
Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen" vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2149; 2001; 3868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

- in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,

- lediglich 24 % der Beschlüsse substanziell begründet werden,

- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann - entgegen häufig gegebener Deutung - nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und

die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z.B. Beweisverwertungsverbote).

- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des - seit Einführung der Vorschrift regelmäßig erweiterten - Straftatenkataloges des § 100 a StPO muss reduziert werden.

- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Gesprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs.2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z.B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Anlage 14: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 21.11.2003
Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15.10.2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung

für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22.10.2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

Anlage 15: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 13.02.2004 Übermittlung von Flugpassagierdaten an die US-Behörden

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z.B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen

Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II – System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet (www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_de.pdf):

Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

Anlage 16: Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.2004 Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

Anlage 17: **Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.2004**
Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

Anlage 18: **Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.2004**
Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z.B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

Anlage 19: **Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.2004**
Radio-Frequency Identification (Übersetzung)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 20.11.2003 an:

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a) sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbe-

zogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b) wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c) dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

d) soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

Anlage 20: Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.2004
Entscheidungen des Bundesverfassungsgerichts vom 03.03.2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 03.03.2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 03.03.2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 03.03.2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

Anlage 21: Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29.10.2004
Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 03.03.2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der

Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 03.03.2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Anlage 22: Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29.10.2004
Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Anlage 23: Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29.10.2004
Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. "Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in

denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

Anlage 24: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26.11.2004
Staatliche Kontenkontrolle muss auf den Prüfstand!

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z.B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z.B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt

weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

Abkürzungsverzeichnis

€	Euro
Abl.	Amtsblatt (der Europäischen Union)
Abs.	Absatz
ADV	Automatisierte Datenverarbeitung
AFGIB	Arbeitsgemeinschaft zur Förderung der Geriatrie in Bayern
AGBSHG	Gesetz zur Ausführung des Bundessozialhilfegesetzes
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
ALKIS	Amtliches Liegenschaftskataster-Informationssystem
AllMBl	Allgemeines Ministerialamtsblatt
Alt.	Alternative
AMD	Arbeitsmedizinischer Dienst
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
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
AZRG	Ausländerzentralregistergesetz
BABY	BZR-Auskunft Bayern
BÄK	Bundesärztekammer
BAQ	Bayerische Arbeitsgemeinschaft für Qualitätssicherung in der stationären Versorgung
BAT	Bundes-Angestelltentarifvertrag
BauGB	Baugesetzbuch
BayArchivG	Bayerisches Archivgesetz
BayBesG	Bayerisches Besoldungsgesetz
BayBG	Bayerisches Beamtengesetz
BayBO	Bayerische Bauordnung
BayBodSchVwV	Verwaltungsvorschrift zum Vollzug des Bodenschutz- und Altlastenrechts in Bayern
BayDAV	Dienstanschlussvorschriften
BayDO	Bayerische Disziplinarordnung
BayDSG	Bayerisches Datenschutzgesetz
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayGlG	Bayerisches Gleichstellungsgesetz
BayHO	Bayerische Haushaltsordnung
BayITSRL	Bayerische IT-Sicherheitsrichtlinien
BayKOM	Bayerisches Kommunikationsnetz
BayKrG	Bayerisches Krankenhausgesetz
BayKRG	Gesetz über das bevölkerungsbezogene Krebsregister Bayern
BayPrG	Bayerisches Pressegesetz
BayPVG	Bayerisches Personalvertretungsgesetz
BayRDG	Bayerisches Rettungsdienstgesetz
BayStatG	Bayerisches Statistikgesetz
BayVBl	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BayVSG	Bayerisches Verfassungsschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BDSG	Bundesdatenschutzgesetz
BEG	Bundesentschädigungsgesetz
BestG	Bestattungsgesetz
BewachV	Verordnung über das Bewachungsgewerbe
BewachVwV	Allgemeine Verwaltungsvorschrift zu § 34 a der GewO und zur Bewachungsverordnung
BFD	Bezirksfinanzdirektion
BfD	Der Bundesbeauftragte für den Datenschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGK	Bayerische Gesundheitschipkarte und Kommunikation
BGSG	Bundesgrenzschutzgesetz
BIOS	Basic Input Output System
BIS	Bodeninformationssystem
bIT4Health	Projekt zur Einführung der elektronischen Gesundheitskarte
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BLKA	Bayerisches Landeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesministerium für Gesundheit
BSHG	Bundessozialhilfegesetz
bspw.	beispielsweise
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz)
BT-Drs.	Bundestagsdrucksache
BtmG	Betäubungsmittelgesetz
BÜVO	Beitragsüberwachungsverordnung
BV	Bayerische Verfassung

BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts (zitiert nach Band und Seite)
BWG	Bundeswahlgesetz
BYBN	Bayerisches Behördennetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
CD-ROM	Compaktdisk – Read Only Memory
CDU	Christlich Demokratische Union
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSU	Christlich Soziale Union
d.h.	das heißt
DAE	Deutsche Arbeitsgemeinschaft für Epidemiologie
DFG	Deutsche Forschungsgemeinschaft
DFK	Digitale Flurkarte
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
DRG	Diagnosis Related Groups
DSB	Datenschutzbeauftragter
DSL	Digital Subscriber Line
DSRV	Datenstelle der Rentenversicherungsträger
DVBl	Deutsches Verwaltungsblatt
DVKRG	Verordnung zur Durchführung des Krebsregistergesetzes
DVMeldeG	Verordnung zur Durchführung des Bayerischen Gesetzes über das Meldewesen
DVWoBindG	Verordnung zur Durchführung des Wohnungsbindungsrechts
E 111	Europäisches Formblatt für Auslandskrankenschein
EA	Errichtungsanordnung für Dateien
EG	Europäische Gemeinschaft
EG-Datenschutzrichtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 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
EuGH	Europäischer Gerichtshof
FAG	Fernmeldeanlagengesetz
FBI	Federal Bureau of Investigation
ff.	folgende
G-10-Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz)
GAnwZ	Geschäftsanweisung für die Geschäftsstellen der Gerichte in Zivilsachen
GAST-Dateien	Dateien zur Gefahrenabwehr und Strafverfolgung
GAZI	Geschäftsanweisung für die Geschäftsstellen der Gerichte in Zivilsachen
GDVG	Gesundheitsdienst- und Verbraucherschutzgesetz
gem.	Gemäß
GEWAN	Gewerbeanzeigen im Netz
GewAnzVwV	Allgemeine Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten Deutschlands
GG	Grundgesetz
ggf.	gegebenenfalls
GiB-DAT-Projekt	Geriatrie-in-Bayern-Datenbank
GKV	Gesetzliche Krankenversicherung
GLA	Geologisches Landesamt
GLKrWG	Gemeinde- und Landkreiswahlgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GMDS	Deutsche Gesellschaft für medizinische Information, Biometrie und Epidemiologie
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GO	Gemeindeordnung
grds.	grundsätzlich
GRUBIS	Grundstücks- und Bodeninformationssystem
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
HPC	Health Professional Card, Heilberufsausweis
HTML	Hypertext Markup Language

HTO	High Tech-Offensive Bayern
i.V.m.	in Verbindung mit
IBP	Informationssystem der Bayerischen Polizei
IfSG	Infektionsschutzgesetz
INPOL	Informationssystem der Polizei (bundesweit)
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITSG	Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung
IuK	Informations- und Kommunikationstechnik
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-KoordR	Richtlinie für die koordinierten Einsatz der Informations- und Kommunikationstechnik (IuK) in der Bayerischen Staatsverwaltung
IuK-Systeme	Informations- und Kommunikationssysteme
JKomG	Justizkommunikationsgesetz
JuMiG	Justizmitteilungsgesetz
JuMoG	Justizmodernisierungsgesetz
JustAG	Justizaktenaufbewahrungsgesetz
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KBV	Kassenärztliche Bundesvereinigung
Kfz	Kraftfahrzeug
KHG	Krankenhausfinanzierungsgesetz
KMBek	Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus
KMS	Schreiben des Bayerischen Staatsministeriums für Unterricht und Kultus
KoA DV	Koordinierungsausschuss Datenverarbeitung
KoA IuK	Koordinierungsausschuss IuK
KORA	Kooperative Gesundheitsforschung in der Region Augsburg
KPMD-PMK	Kriminalpolizeilicher Meldedienst politisch motivierter Kriminalität
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
lit.	Buchstabe
LKrO	Landkreisordnung
LMU	Ludwig-Maximilians-Universität München
LT-Drs.	Landtagsdrucksache
LVA	Landesversicherungsanstalt
LWG	Landeswahlgesetz
m.E.	meines Erachtens
MDK	Medizinischer Dienst der Krankenversicherung
MdL	Mitglied des Landtages
MDStV	Mediendienste-Staatsvertrag
MeldeG	Bayerisches Gesetz über das Meldewesen
MiStra	Anordnung über Mitteilungen in Strafsachen
MiZi	Anordnung über Mitteilungen in Zivilsachen
MSD	Medizinisch-Sozialpädagogische Dienste (Fachdienste bei den Bezirken)
MTArb	Manteltarifvertrag für Arbeiterinnen und Arbeiter des Bundes und der Länder
MWG `92	Münchner Weltwirtschaftsgipfel 1992
Nds.	Niedersächsisch
NGSCB	Next Generation Secure Computing Base
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
o.e.	oben erwähnt
o.g.	oben genannt
ODSP	Online-Datenschutz-Prinzipien
PAG	Bayerisches Polizeiaufgabengesetz
PC	Personalcomputer
PD	Polizeidirektion
PDA	Personal Digital Assistant
PFAD	Personen- und Fall-Auskunfts-datei
PGP	Pretty Good Privacy
PHW	Personenbezogener Hinweis
PID	Patientenidentifikator
PKI	Public Key Infrastructure
PKW	Personenkraftwagen
PP	Polizeipräsidium
PSN	Pseudonym

PStG	Personenstandsgesetz
PSV	Polizeiliche Sachbearbeitung/Vorgangsverwaltung-Verbrechensbekämpfung
PsychThG	Psychotherapeutengesetz
Rdn(r).	Randnummer
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFID	Radio Frequency Identification
ROK	Raumordnungskataster
RSAV	Risikostruktur-Ausgleichsverordnung
RV	RV Rentenversicherung
S.	Seite
s.	siehe
s.o.	siehe oben
S/MIME	Secure Multipurpose Internet Mail Extensions
SDBY	Staatsschutzdatei Bayern
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
sog.	sogenannt
SozhiDAV	Sozialhilfedatenabgleichsverordnung
SPD	Sozialdemokratische Partei Deutschlands
SSC	Security Support Component
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
StVollzG	Strafvollzugsgesetz
TC	Trusted Computing
TCG	Trusted Computing Group
TCM	Trusted Computing Modul
TCPA	Trusted Computer Platform Alliance
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TEMPiS	Telemedizinisches Pilotprojekt zur integrierten Schlaganfallversorgung in der Region Süd-Ost-Bayern
TKG	Telekommunikationsgesetz
TKLGebV	Telekommunikationslizenzgebührenverordnung
TKÜ	Telekommunikationsüberwachung
TMF	Telematikplattform für medizinische Forschungsnetze
TOA	Täter-Opfer-Ausgleich
TÜ	Telefonüberwachung
u.a.	unter anderem
u.U.	unter Umständen
UIG	Umweltinformationsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UrlV	Urlaubsverordnung
USB	Universal Serial Bus
UStG	Umsatzsteuergesetz
UVT	Unfallversicherungsträger
VAwS	Verordnung zum Umgang mit wassergefährdenden Stoffen
VBG 100	Unfallverhütungsvorschrift Arbeitsmedizinische Vorsorge
VDR	Verband Deutscher Rentenversicherungsträger
VersammlG	Versammlungsgesetz
VGemO	Verwaltungsgemeinschaftsordnung
VGH	Verwaltungsgerichtshof
vgl.	Vergleiche
ViCLAS	Violent Crime Linkage Analysis System (Analyse-System zur Verknüpfung von Gewaltverbrechen)
VPN	Virtual Private Network
VSA	VSA Verrechnungsstelle der Süddeutschen Apotheken GmbH
VVWoBindG	Verwaltungsvorschriften zum Vollzug des Wohnungsbindungsgesetzes
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
VwZVG	Verwaltungszustellungs- und Vollstreckungsgesetz
WaffG	Waffengesetz
WLAN	Wireless Local Area Network
WoBindG	Wohnungsbindungsgesetz
WWW	World Wide Web
z.B.	zum Beispiel
ZIL	Zentrale IuK-Leitstelle
ZPO	Zivilprozessordnung
ZSS	Zentrale Speicherstelle
ZStV	Zentrales staatsanwaltschaftliches Verfahrensregister

Stichwortverzeichnis