**Landtag von Baden-Württemberg** **Drucksache 14 / 650**

**14. Wahlperiode** **01. 12. 2006**

# Mitteilung

## des Landesbeauftragten für den Datenschutz

## Siebenundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 1. Dezember 2006:

Anbei übersende ich Ihnen unseren 27. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2006 zu erstatten ist.

Zimmermann

Eingegangen: 01. 12. 2006 / Ausgegeben: 15. 12. 2006

*Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente*

# Siebenundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

## 1. Teil: Zur Situation

„Der Datenschutz hat es derzeit nicht leicht. Wer auf die strikte Beachtung bürgerlicher Freiheitsrechte pocht, macht sich nur wenig Freunde. Schnell gilt man als Bedenkenträger, der den Ernst der Lage nicht erkannt hat. Wer heute dem Publikum gefallen will und Beifall sucht, der muss mit markigen Forderungen auftrumpfen.“ So skizzierte Bundesjustizministerin Brigitte Zypries die augenblickliche Situation des Datenschutzes auf dem 66. Deutschen Juristentag im September dieses Jahres in Stuttgart. Dem ist nicht viel hinzuzufügen. Die nicht zu leugnende terroristische Bedrohung spornt die Fantasie der wirklichen oder auch nur vermeintlichen Sicherheitsfachleute in einer Weise an, dass jegliches Augenmaß verloren zu gehen droht. So meinten einige, den Gefahren des Terrorismus mit dem Einsatz bewaffneter Zugbegleiter begegnen zu können. Wer den Verkehrsalltag kennt, weiß, dass dies Illusion ist. Aber es gibt keine Forderung, die in ihrer Unsinnigkeit nicht noch übertroffen werden könnte. So kamen andere auf die Idee, Hartz-IV-Empfänger in der Zugbegleitung einzusetzen. Was auch immer sonst Motiv für diesen absurden Vorschlag gewesen sein mag, sicherheitspolitisch ist er völlig abwegig. Mit einem „Volkssturm“ gewinnt man nicht den Kampf gegen den Terrorismus.

Hatten diese aktionistischen Vorschläge noch nicht unmittelbar etwas mit dem Datenschutz zu tun, so ging es aber auch bald daran, den Freiheitsrechten der Bürgerinnen und Bürger auf den Pelz zu rücken. Dabei spielt die Forderung nach einer verstärkten Videoüberwachung eine immer größere Rolle. Hierzu später mehr.

Tatsache ist, dass die Terrorismusgefahr zentrales Thema der Sicherheitspolitik auf allen Ebenen war. Dies gilt für den internationalen wie für den nationalen Bereich. Dass dies so ist, ist auch nicht zu beklagen, sondern pure Selbstverständlichkeit. Denn die Sicherheit in einer Gesellschaft ist ein hohes Rechtsgut, so dass die Bürgerinnen und Bürger vom Staat zu Recht einfordern, das ihm Mögliche zur Bekämpfung des Terrorismus zu tun. Dass die Politiker angesichts dieser Forderung nicht untätig erscheinen wollen, liegt nahe. Allerdings täte es vielen Vorschlägen zur Verschärfung staatlicher Eingriffe gut, wenn zunächst einmal geprüft würde, worauf angebliche oder tatsächliche Sicherheitslücken beruhen und ob die bisherigen Befugnisse der Sicherheitsbehörden nicht eigentlich ausreichen. Bei näherer Betrachtung ist nämlich häufig festzustellen, dass Sicherheitslücken eher durch Vollzugsdefizite entstehen und nicht durch unzureichende gesetzliche Grundlagen; die bestehenden Regelungen müssen allerdings auch konsequent angewendet werden. Schließlich ist immer wieder daran zu erinnern, dass der Kampf gegen den Terror nur im Rahmen unserer verfassungsrechtlichen Ordnung, also auch unter Beachtung der bürgerlichen Freiheitsrechte geführt werden kann. Um das Bundesverfassungsgericht zu zitieren: „Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Das schließt nicht nur die Verfolgung des Ziels absoluter Sicherheit aus, welche ohnehin faktisch kaum, jedenfalls nur um den Preis einer Aufhebung der Freiheit zu erreichen wäre. Das Grundgesetz unterwirft auch die Verfolgung des Ziels, die nach den tatsächlichen Umständen größtmögliche Sicherheit herzustellen, rechtsstaatlichen Bindungen, zu denen insbesondere das Verbot unangemessener Eingriffe zählt.“ Auch eine wehrhafte Demokratie verdient diesen Namen nur, wenn sie rechtsstaatlich bleibt. Dass die sich hieraus ergebenden Grenzen stets eingehalten werden, begegnet zunehmend ernsten Zweifeln.

Auf internationaler Ebene hat im Berichtsjahr die Behandlung von Fluggastdaten eine große Rolle gespielt. Das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das US-Ministerium für Heimatschutz vom Mai 2004 hatte erhebliche Mängel beim Datenschutz offenbart. Die Datenschutzbeauftragten des Bundes und der Länder hatten schon in ihrer Entschließung vom 13. Februar 2004 zur Übermittlung von Flugpassagierdaten an die US-Behörden (vgl. 25. Tätigkeitsbericht, LT-Drucksache 13/3800) darauf hingewiesen, dass das Abkommen den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte gewähre. Auch die Anforderungen, die die Gruppe nach Artikel 29 der Europäischen Datenschutzrichtlinie, ein unabhängiges europäisches Beratungsgremium in

Datenschutzfragen, insbesondere an den Umfang der zu übermittelnden Daten, die Dauer ihrer Speicherung und die Art ihrer Verwendung gestellt hatte, waren nur teilweise berücksichtigt. Der Gerichtshof der Europäischen Gemeinschaften erklärte mit Urteil vom 30. Mai 2006 das bisherige Abkommen im Ergebnis wegen fehlender Rechtsgrundlage für nichtig. Die Hoffnungen richteten sich deshalb auf das notwendig gewordene zweite Abkommen, das schließlich am 19. Oktober 2006 zustande kam. Der Schutz von Fluggastdaten ist durch dieses zweite Abkommen jedoch kaum gestärkt worden, da es inhaltlich im Wesentlichen unverändert blieb.

Nach dem neuen Abkommen dürfen die US-Behörden bei Flügen zwischen der Europäischen Union und den Vereinigten Staaten weiterhin unmittelbar Daten aus den Buchungs- und Abfertigungssystemen der Fluggesellschaften abrufen („Pull-Verfahren“); das gilt so lange, bis ein technisches System zur Verfügung steht, das es den Fluggesellschaften ermöglicht, die Daten selbst den US-Behörden zu übermitteln („Push-Verfahren“). Zu den abrufbaren Daten gehören neben dem Namen und der Anschrift des Passagiers unter anderem das Datum der Reservierung, die Zahlungsart, die Telefonnummern, das Reisebüro, die E-Mail-Adresse, die Sitzplatznummer, etwaige Essenswünsche, die Historie über nicht angetretene Flüge, die Zugehörigkeit zu einem Vielfliegerprogramm und die Zahl der Gepäckstücke. Nicht abschließend geklärt sind weiterhin die zulässige Speicherdauer der Daten, die zulässigen Verwendungszwecke und – was notwendige Grundlage für eine zulässige Datenweitergabe ist – die Eignung der Daten für die Bekämpfung des Terrorismus. Es bleibt zu hoffen, dass es der Europäischen Union möglichst bald gelingt, ein Abkommen abzuschließen, das die personenbezogenen Daten der Fluggäste hinreichend schützt. Unabhängig davon können Flugreisende ihre Daten durch die entsprechende Auswahl ihres Flugziels auch selbst schützen, sofern sie, wie etwa bei Urlaubsreisen, eine Wahlmöglichkeit haben.

Im nationalen Bereich sind in diesem Zusammenhang zwei Gesetzesvorhaben des Bundes zu nennen: Das Gemeinsame-Dateien-Gesetz, in dessen Mittelpunkt die Schaffung einer gemeinsamen Antiterrordatei für Polizei und Nachrichtendienste steht, sowie das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes, mit dem nach den Anschlägen vom 11. September 2001 geschaffene Befugnisse von Polizei und Nachrichtendiensten fortgeschrieben und teilweise erweitert werden sollen. Insbesondere die geplante Antiterrordatei, die zwischen den Innenministern von Bund und Ländern Anfang September 2006 verabredet wurde, ist aus mehreren Gründen datenschutzrechtlich bedenklich: Sie droht die unterschiedlichen Aufgaben und Befugnisse von Polizei und Nachrichtendiensten in verfassungsrechtlich bedenklicher Weise zu vermischen, erlaubt zu vielen Polizeidienststellen den Zugriff auf die Datei, erfasst zu viele Daten und zieht den Kreis der einzuspeichernden Personen zu weit. Außerdem fehlen klare und spezifische Regelungen über Berichtigung, Änderung und Löschung der Daten. Insgesamt zeichnen sich bei der Antiterrordatei ähnliche Probleme ab, wie sie auf Landesebene bereits mit der „Arbeitsdatei Politisch motivierte Kriminalität“ zu beobachten sind (vgl. 26. Tätigkeitsbericht, LT-Drucksache 13/4910, und in diesem Bericht, 2. Teil, 1. Abschnitt, Nr. 4). Im Zuge der Befassung des Bundesrats hat Baden-Württemberg sogar für weitere Verschärfungen plädiert und erreicht, dass sich der Bundesrat für eine Aufhebung der von der Bundesregierung vorgesehenen Befristung des Gesetzes ausgesprochen hat. Es bleibt zu hoffen, dass der Bundestag diesen überzogenen Forderungen eine Absage erteilt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich auf ihrer Sitzung am 26./27. Oktober 2006 ebenfalls mit der geplanten Antiterrordatei befasst und auf schwerwiegende verfassungs- und datenschutzrechtliche Risiken hingewiesen. Die von der Konferenz verabschiedete Entschließung ist diesem Bericht als Anhang 1 angeschlossen.

Das Terrorismusbekämpfungsgesetz vom 9. Januar 2002, das die Befugnisse der Nachrichtendienste erheblich erweitert hatte, enthielt teilweise auf fünf Jahre befristete Regelungen. Die Bundesregierung hat deshalb zunächst das geltende Gesetz evaluiert und anschließend den Entwurf eines Ergänzungsgesetzes vorgelegt, mit dem nicht nur die befristeten Regelungen erneut verlängert, sondern zugleich einige nicht unwesentliche Ergänzungen vorgenommen werden sollen. Insbesondere sollen die Auskunftsbefugnisse der Nachrichtendienste erweitert werden und sich jetzt sogar auf den gewaltbereiten Extremis-

mus und auf Propagandaaktivitäten erstrecken können. Ferner sollen Befugnisse, die bislang dem Verfassungsschutz vorbehalten sind, pauschal auf den Bundesnachrichtendienst und den Militärischen Abschirmdienst übertragen werden (z. B. bei der Abfrage von Telekommunikationsdaten und von Nutzungsdaten des Internets). Außerdem sollen einige verfahrensrechtliche Hürden abgesenkt werden. Bereits die Ausgangsprämisse, dass sich das Terrorismusbekämpfungsgesetz von 2002 bewährt habe, ist kritisch zu hinterfragen. Zum einen hat die Bundesregierung die Bewertung des Gesetzes ohne neutrale Gutachter selbst vorgenommen, zum anderen waren die Fallzahlen teilweise so gering, dass eine Verlängerung der entsprechenden Befugnisse fragwürdig erscheint. Immerhin ist erfreulich, dass nunmehr eine Evaluierung des Terrorismusbekämpfungsergänzungsgesetzes unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, vorgesehen ist. Eine ähnliche Regelung soll übrigens auch das Gemeinsame-Dateien-Gesetz erhalten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 26./27. Oktober 2006 die aktuellen Antiterrorgesetze zum Anlass genommen, an die notwendige Balance zwischen Freiheit und Sicherheit zu erinnern. Aus Sicht des Datenschutzes zeichne sich eine Entwicklung ab, wonach der Staat sich immer mehr zu einem Präventionsstaat wandele, der seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr verlagere und mit seinen Maßnahmen eine Vielzahl unverdächtiger Menschen erfasse. Dieses neue Verständnis von innerer Sicherheit führe zu gravierenden Einschränkungen der Freiheitsrechte. Die vollständige Entschließung der Datenschutzbeauftragten ist diesem Bericht als Anhang 2 beigefügt.

Das Bundesverfassungsgericht hat seinerseits – wieder einmal – an die Grenzen einer zu übereifrigen Sicherheitsgesetzgebung erinnern müssen. Mit seiner Entscheidung zur Rasterfahndung hat es die verfassungsrechtlichen Maßstäbe wieder zurechtgerückt. Nach dem Beschluss vom 4. April 2006, 1 BvR 518/02, war die präventiv-polizeiliche Rasterfahndung auf der Grundlage des nordrhein-westfälischen Polizeigesetzes nicht verfassungsgemäß. Die erforderliche „konkrete Gefahr für hochrangige Rechtsgüter“ habe nicht vorgelegen. Aus dieser Entscheidung ergibt sich für den Landesgesetzgeber meines Erachtens die Notwendigkeit, über die nicht verfassungskonformen Bestimmungen zur Rasterfahndung im baden-württembergischen Polizeigesetz hinaus auch andere Vorschriften anzupassen; damit meine ich insbesondere polizeirechtliche Regelungen, durch die eine Vielzahl unbeteiligter Personen von polizeilichen Maßnahmen betroffen werden. Für die angekündigte Novelle des Polizeigesetzes hat das Bundesverfassungsgericht mit seiner wegweisenden Entscheidung zur Rasterfahndung jedenfalls einige beachtliche Hürden aufgerichtet.

Auch die Politik auf Landesebene hat in der Sicherheitsdiskussion kräftig mitgemischt. Schon bald nach den fehlgeschlagenen Anschlägen auf zwei Regionalzüge der Deutschen Bahn Ende Juli dieses Jahres kündigte der Innenminister eine umfassende Novellierung des Polizeigesetzes an. Wie der Presse zu entnehmen war, ist wohl u. a. daran gedacht, eine rechtliche Grundlage für den Einsatz automatisierter Lesesysteme von Kraftfahrzeugkennzeichen zu schaffen, die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts zur Rasterfahndung umzusetzen und insbesondere die Videoüberwachung erheblich auszuweiten. Da ein entsprechender Gesetzentwurf hier noch nicht bekannt ist, kann ich auf Einzelheiten der beabsichtigten Regelungen naturgemäß noch nicht eingehen. Weil sich die Meldungen zur Verstärkung der Videoüberwachung aus dem Innenministerium in den Medien förmlich überschlagen haben, sind hierzu aber doch einige allgemeine Anmerkungen angebracht.

Im Innenministerium scheinen sehr konkrete Vorstellungen darüber zu bestehen, in welcher Weise die polizeiliche Videoüberwachung ausgebaut werden soll. Da es sich hierbei um sehr weit reichende Eingriffe in die Persönlichkeitsrechte der Bürgerinnen und Bürger handeln dürfte, hätte ich es sehr begrüßt, wenn das Innenministerium schon frühzeitig – also schon bevor ein offizieller Gesetzentwurf präsentiert wird – die Abstimmung mit dem Landesdatenschutzbeauftragten gesucht hätte. Dies ist bislang leider unterblieben, obwohl sich in der Vergangenheit bei anderen Projekten eine frühzeitige Einschaltung des Landesbeauftragten aus meiner Sicht bewährt hat.

Zur Sache selbst: Offensichtlich sieht das Innenministerium in der Videoüberwachung einen tragenden Pfeiler der Terrorismusbekämpfung. Diese Erwartung muss jedoch stark relativiert werden. Wenn auch unbestritten ist, dass die Videoüberwachung zur Aufklärung bereits geschehener Anschläge wertvolle Hilfsdienste leisten kann, so sind sich Fachleute doch darin einig, dass die Videoüberwachung nicht dazu geeignet ist, geplante terroristische Anschläge zu verhindern. Für das klassische Aufgabengebiet des Polizeirechts – die Gefahrenabwehr – ist die Videoüberwachung jedenfalls im Zusammenhang mit der Terrorismusbekämpfung daher ein ungeeignetes Mittel. Wenn auf den Präventionswert der Videoüberwachung hingewiesen wird, mag dies für die gewöhnliche Straßenkriminalität eine gewisse Berechtigung haben; Terroristen aber, die auch eine Selbsttötung in Kauf nehmen, lassen sich durch eine Videoüberwachung in keiner Weise von ihrem Tun abhalten. Das Gefahrenabwehrrecht spielt demnach im Zusammenhang mit Videoüberwachung und Terrorismusbekämpfung keine Rolle. Eine Lockerung der polizeigesetzlichen Voraussetzungen für die Videoüberwachung zur Terrorismusbekämpfung macht daher rechtlich keinen Sinn.

Im Übrigen ist nach den bisherigen Verlautbarungen des Innenministeriums noch völlig unklar, wie dies rechtstechnisch geschehen soll. Es ist die Rede von einer neuen polizeirechtlichen Gefahrenkategorie, der sog. „einfachen Gefahr“, bei der künftig eine polizeiliche Videoüberwachung bereits zulässig sein soll. Unabhängig davon, was eine solche „einfache Gefahr“ überhaupt sein soll, ist in diesem Zusammenhang auf Folgendes hinzuweisen: Zum einen hat bereits der VGH Mannheim in seiner Entscheidung zu der in Mannheim praktizierten Videoüberwachung unmissverständlich festgestellt, dass eine Videoüberwachung zur Gefahrenabwehr geeignet und erforderlich und die Abgrenzung der beobachteten Örtlichkeit bestimmt genug sein muss. Der als Anknüpfungspunkt ins Gespräch gebrachte Begriff einer „größeren Ansammlung von Menschen“ dürfte diesem Bestimmtheitserfordernis nicht genügen. Zum anderen ist an die jüngste Rechtsprechung des Bundesverfassungsgerichts zur Rasterfahndung zu erinnern; das Bundesverfassungsgericht hat hier als Eingriffsschwelle das Vorliegen einer „konkreten Gefahr“ verlangt. Es dürfte naheliegen, dass bei dem in der Schwere zumindest vergleichbaren Eingriff in das Persönlichkeitsrecht einer Vielzahl unbeteiligter Personen durch eine Videoüberwachung aus verfassungsrechtlichen Gründen Vergleichbares zu fordern ist.

Bemerkenswert ist, dass Baden-Württemberg in Sachen Videoüberwachung offenbar noch über das hinausgehen will, was die Innenministerkonferenz für sachgerecht ansieht. Diese hatte beschlossen, im Bereich von Bahnhöfen, Flughäfen und Häfen die Möglichkeiten der Videoüberwachung stärker zu nutzen. Im Innenministerium dagegen ist jetzt sogar die Rede von einem „Video-Atlas“, auf dessen Grundlage sich die Polizei die private Videoüberwachung, z. B. bei Banken, Tankstellen und Einkaufspassagen, umfassend für eigene Zwecke zunutze machen will. Schon der Begriff wirkt verheerend, weil er – ob gewollt oder ungewollt – suggeriert, dass die polizeiliche Videoüberwachung je nach Bedarf und an nahezu jedwedem Ort möglich werden soll. Auch dem Innenministerium dürfte allerdings klar sein, dass eine polizeiliche Videoüberwachung nicht überall dort zulässig ist, wo eine private Überwachung stattfindet. Die Polizei kann private Betreiber nicht einfach zum verlängerten Arm in jenen Bereichen machen, wo sie selbst nicht tätig werden darf. Die offensichtlich angestrebte Vereinbarung mit den privaten Betreibern für eine polizeiliche „Aufschaltung“ macht eine wirksame Rechtsgrundlage für die polizeiliche Videoüberwachung im Polizeigesetz nicht entbehrlich. Und die verfassungsrechtliche Schwelle hierfür ist – wie oben ausgeführt – beachtlich. Insgesamt sollte sich das Innenministerium fragen, ob die derzeit im Polizeigesetz verankerten Regelungen zur Videoüberwachung für Zwecke der Gefahrenabwehr nicht völlig ausreichen. Schließlich ist auch daran zu erinnern, dass die Polizei in einem strafrechtlichen Ermittlungsverfahren bei Bedarf auch private Videoaufzeichnungen beschlagnahmen darf, was für die Zwecke der Strafverfolgung ausreichen sollte. Offensichtlich liegen die Hemmnisse in der Umsetzung der Überwachungsmöglichkeiten etwa bei Kriminalitätsbrennpunkten auch weniger an einer zu eng gefassten Rechtsgrundlage als vielmehr an dem für Videoüberwachungs-Maßnahmen erforderlichen Personalaufwand, der beträchtlich ist. Wenn beabsichtigt sein sollte, diesen Aufwand mit der neuen Konzep-

tion auf elegante Weise auf private Betreiber abzuwälzen, so wird diese Rechnung nicht aufgehen. Denn die Polizei kann sich ihrer Pflicht, Gefahrensituationen im Zuge einer Videoüberwachung selbst zu erkennen, um entsprechende Abwehrmaßnahmen einleiten zu können, nicht durch schlichtes Abwälzen der Videoüberwachungs-Tätigkeit auf Private entledigen.

Nach alledem birgt die beabsichtigte Novellierung des Polizeigesetzes einige Brisanz. Die Arbeiten an der Novelle werden eine Nagelprobe für die Frage sein, wie es das Land mit der Beachtung der bürgerlichen Freiheitsrechte hält. In diesem Zusammenhang kann nochmals die Bundesjustizministerin zitiert werden, die auf dem jüngsten Deutschen Juristentag an Folgendes erinnerte: „Unsere Grundrechte, und dazu gehört auch das Recht auf informationelle Selbstbestimmung, bleiben der Maßstab und die Grenze der Staatsgewalt. Trotz neuer Risiken gilt: Der Zweck heiligt nicht alle Mittel.“

# 2. Teil: Öffentliche Sicherheit und Ordnung

## 1. Abschnitt: Öffentliche Sicherheit

### 1. Die Ausschreibung zur verdeckten Registrierung nach Artikel 99 des Schengener Durchführungsübereinkommens

Wenn jemand von der Polizei angehalten und kontrolliert wird, zum Beispiel bei Verkehrskontrollen oder beim Grenzübertritt, dann muss er in der Regel Ausweisdokumente vorlegen, deren Daten mit den Daten in einem Polizeicomputer abgeglichen werden. Was viele nicht wissen: Bei diesen Überprüfungen geht es nicht nur um die Suche nach alkoholisierten Verkehrsteilnehmern oder die Fahndung nach zur Festnahme ausgeschriebenen Verbrechern. In manchen Fällen ist die Polizei nur daran interessiert zu erfahren, wo sich jemand gerade aufhält, mit wem er zusammen im Auto unterwegs ist oder wo er gerade herkommt. Die Beobachtungen der Polizei werden dann – ohne dass der Betroffene etwas davon mitbekommt – an die ausschreibende Polizeidienststelle gemeldet. Diese Maßnahme wird im Polizeigesetz des Landes (§ 25 PolG) als „Mitteilung über das Antreffen von Personen“ bezeichnet, in den Polizeigesetzen anderer Bundesländer und in der polizeilichen Praxis ist der Begriff „polizeiliche Beobachtung“ üblich, auf der europäischen Ebene – genauer: in den Mitgliedstaaten des Schengener Übereinkommens – heißt sie „verdeckte Registrierung“. Hiermit haben wir uns im Jahr 2006 eingehend befasst.

Das Schengener Übereinkommen und dessen Auswirkungen auf die Zusammenarbeit der Sicherheitsbehörden in Europa waren bereits wiederholt Gegenstand unserer Berichterstattung (vgl. 21. Tätigkeitsbericht, LT-Drucksache 12/5740, und 24. Tätigkeitsbericht, LT-Drucksache 13/2650). Kernstück des Abkommens ist das Schengener Informationssystem (SIS), eine riesige Datenbank für mittlerweile praktisch alle europäischen Staaten, deren Zentralrechner in Straßburg steht. In dieser Datenbank sind zahlreiche Personen aus allen möglichen Gründen ausgeschrieben, zum Beispiel zur Festnahme, zur Verweigerung der Einreise oder aber zur verdeckten Registrierung. Mit der verdeckten Registrierung soll – wie gesagt – bei Gelegenheit von Polizeikontrollen festgestellt werden, wo sich die betreffende Person aufhält, mit welchem Fahrzeug sie unterwegs und mit wem sie zusammen ist, möglichst auch wohin sie aus welchem Grund reist. Kurzum, die heimliche, eben „verdeckte“ Registrierung wird stets dann angeordnet, wenn ein Bewegungs- und Verhaltensprofil über die ausgeschriebene Person erstellt werden soll. Die Polizeibeamten der Schengener Vertragsstaaten, die bei einer Kontrolle nach einem Blick in den Computer feststellen, dass sie es mit einer ausgeschriebenen Person zu tun haben, haben den Betroffenen so unauffällig wie möglich auszuforschen und die erhobenen Daten dann derjenigen Polizeidienststelle in einem anderen Mitgliedstaat zu übermitteln, die den Betreffenden zur verdeckten Registrierung ausgeschrieben hat. Auf diese Weise ergibt sich mit der Zeit eine Übersicht über die Reisewege und die Begleiter der ausgeschriebenen Person sowie die von ihr benutzten Fahrzeuge.

Zwar ist diese Art der polizeilichen Überwachung nicht so intensiv wie die permanente verdeckte Observation des Betroffenen und erfolgt zwangsläufig nur punktuell, nämlich nur dann, wenn aus einem anderen Grund eine polizeiliche Kontrolle stattfindet, aber auch die Ausschreibung zur verdeckten Registrierung stellt einen gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Es versteht sich daher von selbst, dass die Ausschreibung für diesen Zweck nicht für die Beobachtung von Kleinkriminellen in Frage kommt, sondern nur zur Aufklärung oder Verhinderung gewichtiger Straftaten gedacht ist. Dementsprechend sieht Artikel 99 des Schengener Durchführungsübereinkommens (SDÜ), in dem u. a. die Nutzung des Schengener Informationssystem geregelt ist, vor, dass eine Ausschreibung zur verdeckten Registrierung (nur) dann zur Strafverfolgung oder zur Abwehr von Gefahren für die öffentliche Sicherheit zulässig ist, wenn entweder (a) konkrete Anhaltspunkte dafür vorliegen, dass der Betroffene in erheblichem Umfang außergewöhnlich schwere Straftaten plant oder begeht, oder aber (b), wenn die Gesamtbeurteilung des Betroffenen,

insbesondere aufgrund der bisher von ihm begangenen Straftaten, erwarten lässt, dass er auch künftig außergewöhnlich schwere Straftaten begehen wird. Die Vertragsstaaten haben also recht hohe Hürden aufgerichtet, bevor jemand überhaupt zur verdeckten Registrierung in fast ganz Europa ausgeschrieben werden kann. Es reicht jedenfalls keine allgemeine polizeiliche Neugier aus, den aktuellen Aufenthaltsort einer verdächtigen Person in Erfahrung zu bringen, sondern es müssen Straftaten von erheblichem Kaliber in Rede stehen. Wenn die betreffende Person sich bisher noch nicht strafbar gemacht hat (Variante a), müssen sogar konkrete Anhaltspunkte – also nicht nur vage Verdachtsmomente – dafür vorliegen, dass der Betreffende in erheblichem Umfang straffällig zu werden droht.

Das baden-württembergische Polizeigesetz legt die Messlatte etwas tiefer: Nach § 25 PolG kann eine Person oder ihr Fahrzeug zum Zwecke der „Mitteilung über das Antreffen“ ausgeschrieben werden (im polizeilichen Informationssystem des Landes – POLAS-BW – oder im polizeilichen Informationssystem von Bund und Ländern – INPOL-Z), wenn entweder die Gesamtwürdigung der Person und ihrer bisher begangenen Straftaten erwarten lässt oder Tatsachen die Annahme rechtfertigen, dass die betreffende Person künftig Straftaten mit erheblicher Bedeutung (§ 22 Abs. 5 PolG) begehen wird und die Mitteilung über das Antreffen der Person zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist. Straftaten mit erheblicher Bedeutung sind danach Verbrechen und bestimmte Vergehen, die im Einzelfall nach Art und Schwere geeignet sein müssen, den Rechtsfrieden besonders zu stören. Der nur auf den ersten Blick eindeutige Straftatenkatalog in § 22 Abs. 5 PolG erweist sich bei näherer Betrachtung als reichlich unübersichtlich und unscharf, da auf weitere Vorschriften verwiesen wird und zum Beispiel auch „gewohnheitsmäßig“ oder „sonst organisiert“ begangene Vergehen als „Straftaten von erheblicher Bedeutung“ angesehen werden (§ 22 Abs. 5 Buchst. c PolG). Immerhin dürfte klar sein, dass die für eine Ausschreibung im Schengener Informationssystem geforderten „außergewöhnlich schweren Straftaten“ gewichtiger sein müssen als die nach Landesrecht erforderlichen „Straftaten von erheblicher Bedeutung“. Wie sich bei einer konzertierten Kontrollaktion der europäischen Datenschutzbeauftragten im Sommer 2006 herausgestellt hat, hat die baden-württembergische Polizei die unterschiedlichen Voraussetzungen nicht immer beachtet.

Die Gemeinsame Kontrollinstanz nach Artikel 115 SDÜ hatte nämlich eine gemeinsame Kontrolle des Verfahrens der Ausschreibungen nach Artikel 99 SDÜ in allen Schengen-Vertragsstaaten beschlossen, nachdem sie festgestellt hatte, dass die Anzahl dieser Ausschreibungen in den Vertragsstaaten erheblich voneinander abwich; in manchen Ländern wurde das Verfahren offenbar überhaupt nicht genutzt. Hierdurch wird natürlich der Sinn des Datenverbunds generell in Frage gestellt. Von den deutschen Behörden waren zum Stichtag 19. Januar 2006 immerhin 1 104 Personen zur verdeckten Registrierung nach Artikel 99 SDÜ ausgeschrieben worden. Das Bundesinnenministerium lieferte außerdem Zahlen, wie sich die Anordnungen auf die einzelnen Bundesländer verteilten. Dabei ergaben sich kaum erklärbare Unterschiede: So wiesen beispielsweise Baden-Württemberg 376 und Bayern 348, Hessen hingegen nur 67, Niedersachsen nur 18, Nordrhein-Westfalen 83 und Rheinland-Pfalz 26 Ausschreibungen nach Artikel 99 SDÜ zum genannten Stichtag auf.

Um herauszufinden, warum Baden-Württemberg überdurchschnittlich viele Ausschreibungen zur verdeckten Registrierung in den Schengen-Staaten veranlasst hatte, führten wir eine Prüfung beim Landeskriminalamt Baden-Württemberg durch, das die Ausschreibungsanträge der einzelnen Polizeidienststellen bearbeitet und die Ausschreibungen im Staatsschutzbereich selbst zentral umsetzt. Das Landeskriminalamt nannte uns zum Vergleich auch die Gesamtzahlen der Ausschreibungen zur polizeilichen Beobachtung bzw. verdeckten Registrierung in den nationalen Systemen INPOL-Z und POLAS-BW bzw. im Schengener Informationssystem (Stand: 23. Mai 2006); diese Übersicht ergab erneut erstaunliche Unterschiede: Baden-Württemberg hatte insgesamt 468, Hessen 200, Niedersachsen 142, Nordrhein-Westfalen 269, Rheinland-Pfalz 51 und Bayern sogar 2 208 Ausschreibungen veranlasst. Während in Baden-Württemberg demnach rund 80 % aller Ausschreibungen zusätzlich in dem europäischen Fahndungssystem (SIS) vorgenom-

men wurden, waren dies in Bayern „nur“ rund 15 %. Sollte die Bedeutung der internationalen Ausschreibung zur verdeckten Registrierung so unterschiedlich eingeschätzt werden?

Der Vollständigkeit halber ist noch zu erwähnen, dass die nach Artikel 99 SDÜ ebenfalls mögliche „Ausschreibung zur gezielten Kontrolle“ im nationalen Recht nicht vorgesehen ist, so dass die entsprechende Ausschreibung einer ausländischen Polizeibehörde automatisch in eine Ausschreibung zur verdeckten Registrierung umgewandelt wird (Artikel 99 Abs. 5 Satz 2 SDÜ).

Das Landeskriminalamt erklärte die vergleichsweise hohe Anzahl der Ausschreibungen nach Artikel 99 SDÜ in Baden-Württemberg bzw. den hohen Anteil dieser Ausschreibungen an der Gesamtzahl aller Ausschreibungen zur polizeilichen Beobachtung u. a. damit, dass nach der einschlägigen Polizeidienstvorschrift eine polizeiliche Beobachtung mindestens bundesweit stattfinden solle, eine Ausdehnung auf die Schengen-Staaten stets zu prüfen und außerdem eine größtmögliche räumliche Ausdehnung der Ausschreibung anzustreben sei. Die nachgeordneten Dienststellen würden angehalten, diese Kriterien zu beachten. Eine Ausschreibung zur polizeilichen Beobachtung würde daher nur dann nicht auf die Schengen-Staaten ausgedehnt, wenn die betreffende Zielperson eindeutig nur regional aufgetreten sei. Allerdings sei eine aus der Ausschreibung nach Artikel 99 SDÜ folgende Einspeicherung der betreffenden Person im Schengener Informationssystem gegenüber der Einspeicherung in den polizeilichen Informationssystemen des Bundes bzw. des Landes auf der Grundlage des nationalen Rechts subsidiär, da für eigene Zwecke die nationalen Systeme ausreichten. Insofern bestehe ein echter Zusatznutzen eigentlich „nur“ für ausländische Dienststellen. Dies erkläre möglicherweise auch die vergleichsweise niedrigen Ausschreibungszahlen in anderen Bundesländern. Das Landeskriminalamt wies ferner darauf hin, dass in der Aufstellung auch einige Ausschreibungen durch Justizbehörden nach § 163 e der Strafprozessordnung (StPO) enthalten seien, die wir bei unseren weiteren Nachforschungen ausklammerten.

Bei der Durchsicht der Gesamtliste der Anordnungen nach Artikel 99 SDÜ in Baden-Württemberg fiel zunächst auf, dass bei zahlreichen Maßnahmen die Begründung gleich lautend und die den Antrag stellende Dienststelle identisch waren und dass jeweils mehrere Personen betroffen waren, dass also ein bandenmäßiger oder organisierter Tatzusammenhang zu vermuten war. Den „Spitzenreiter“ in dieser Hinsicht bildete die Einspeicherung von 63 überwiegend minderjährigen Personen durch die Ermittlungsgruppe „Mobile Kinderbanden“ beim Regierungspräsidium (Landespolizeidirektion) Karlsruhe; für diese Zielgruppe liefen die Maßnahmen allerdings teilweise Anfang Juni 2006 wieder aus. Etliche Personen waren auch von der Beobachtung von Rockerbanden (teilweise bis zu 24 Betroffene) und in- und ausländischen Banden, die der Begehung von Eigentumsdelikten verdächtigt wurden, betroffen. Gemeinsame Tatzusammenhänge lagen auch vielen Anordnungen aus dem Staatsschutzbereich zugrunde, die überwiegend auf die Erkenntnisgewinnung bezüglich (mutmaßlich) islamistischer Gruppierungen gerichtet waren und daher jeweils mehrere Angehörige einer Gruppe betrafen.

Die Gesamtliste enthielt zahlreiche „Altfälle“, bei denen die erste Anordnung teilweise schon mehrere Jahre zurücklag. Hierzu ist anzumerken, dass sowohl die Ausschreibung zur verdeckten Registrierung nach Artikel 99 SDÜ wie auch die Ausschreibung zum Zweck der Mitteilung über das Antreffen einer Person nach § 25 PolG zeitlich auf höchstens zwölf Monate zu befristen sind (Artikel 112 Abs. 1 Satz 3 SDÜ bzw. § 25 Abs. 2 Satz 2 PolG), wobei neu anzuordnende Verlängerungen bis zu jeweils zwölf Monate zulässig sind. Ferner ist die Ausschreibung unverzüglich zu löschen, wenn deren Voraussetzungen nicht mehr vorliegen oder der Zweck der Ausschreibung erreicht worden ist bzw. nicht mehr erreicht werden kann (§ 25 Abs. 3 PolG). Schließlich ist der Betroffene nach Beendigung der Maßnahme zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann (Artikel 109 SDÜ bzw. § 25 Abs. 4 in Verbindung mit § 22 Abs. 8 PolG). Wenn man sich vor Augen hält, dass die polizeiliche Beobachtung zum einen nur bei gravierendem Straftatverdacht Anwendung finden kann, zum andern aber nur punktuelle „Zufallserkenntnis-

se“ liefert, dann wird deutlich, dass die polizeiliche Beobachtung eigentlich immer nur ein „Durchgangsstadium“ zwischen dem unverdächtigen, für die Polizei nicht relevanten Verhalten und dem Vorliegen eines Anfangsverdachts, der zur Einleitung eines strafrechtlichen Ermittlungsverfahrens zwingt, abbildet. Eigentlich gibt es bei einer Verlängerung der Ausschreibung nur zwei Alternativen: Entweder hat sich im zurückliegenden Anordnungszeitraum der Verdacht einer drohenden Straftat von erheblicher Bedeutung (nach nationalem Recht, § 25 PolG) bzw. einer drohenden außergewöhnlich schweren Straftat (nach Maßstab von Artikel 99 SDÜ) bestätigt oder sogar verstärkt; dann muss die Polizei eigentlich zu intensiveren Maßnahmen greifen und beispielsweise die verdächtige Person permanent observieren, um endlich ein strafrechtliches Ermittlungsverfahren einleiten zu können. Oder aber der ursprüngliche Verdacht bestätigt sich nicht und die polizeiliche Beobachtung liefert keine zusätzlichen Erkenntnisse, die das Ermittlungsverfahren näherrücken lassen, dann kann die Beobachtung nicht uferlos fortgesetzt werden in der Hoffnung, irgendwann doch noch einen Zufallstreffer zu landen. So gesehen, sind an die Verlängerung einer Anordnung nach Artikel 99 SDÜ bzw. § 25 PolG strenge Anforderungen zu stellen. Um festzustellen, ob diese Anforderungen erfüllt wurden, haben wir uns zunächst auf die „Altfälle“ konzentriert.

Aus den „Altfällen“ haben wir die Vorgänge ausgewählt, bei denen die erstmalige Anordnung zur Ausschreibung nach Artikel 99 SDÜ vor mehr als zwei Jahren erfolgte. Hierbei ergaben sich 62 Fälle, die zu unserer Überraschung allesamt den Staatsschutzbereich betrafen (sog. PB 07-Fälle); diese Fälle haben wir dann zuerst in Augenschein genommen. Im Staatsschutzbereich verfügt das Landeskriminalamt wegen der zentralen Bearbeitung dieser Fälle jeweils über die vollständigen Unterlagen. Um einen Überblick über Maßnahmen außerhalb des Staatsschutzbereichs zu gewinnen – die maßgebliche Polizeidienstvorschrift nennt insgesamt elf Kategorien –, wurden aus der Gesamtliste nach dem Zufallsprinzip weitere 56 Fälle ausgewählt, zu denen die im Landeskriminalamt vorhandenen Unterlagen (im Wesentlichen Anordnung der Maßnahme, Antrag mit Begründung, ggf. Schriftwechsel zwischen Dienststelle und Landeskriminalamt) geprüft wurden. In diesen Fällen befanden sich die Unterlagen bei der sachbearbeitenden Dienststelle, die auch den Antrag auf Anordnung der polizeilichen Beobachtung an das Landeskriminalamt gerichtet hatte. Eine Akteneinsicht bei den sachbearbeitenden Dienststellen erfolgte aus arbeitsökonomischen Gründen nicht. Die Plausibilität der Anordnungen konnte jedoch – wie der Vergleich mit den Staatsschutzfällen ergab – anhand der beim Landeskriminalamt vorhandenen Unterlagen hinreichend beurteilt werden.

Zum Ausschreibungsverfahren ist noch Folgendes zu sagen: Die Ausschreibung nach Artikel 99 SDÜ wird nach Maßgabe des nationalen Rechts von der dafür zuständigen Stelle ausgesprochen: Sofern es sich um eine (präventive) Ausschreibung zur Gefahrenabwehr bzw. vorbeugenden Straftatenbekämpfung handelt, wird sie vom Leiter des Landeskriminalamts oder von einem von ihm besonders beauftragten Polizeibeamten des höheren Dienstes angeordnet (§ 25 Abs. 2 Satz 1 PolG). Sofern es sich um eine Ausschreibung zur Strafverfolgung handelt, ist sie vom Richter, bei Gefahr im Verzug auch von der Staatsanwaltschaft anzuordnen (§ 163 e Abs. 4 StPO). Die Einleitung der Fahndung geschieht technisch in der Weise, dass die jeweilige Justizbehörde bzw. Polizeidienststelle das hierfür vorgesehene Fahndungsformular (KP 21/24) ausfüllt, dabei die Fahndung als „Schengen-Fahndung“ durch Ankreuzen des Feldes „SIS“ kennzeichnet und das Formular an die zuständige Datenstation weiterleitet, die den Datensatz in INPOL eingibt. Diese aktiviert in der Eingabemaske von INPOL das Feld „FSI“ durch den Buchstaben „A“ (aktiviert) und steuert hierdurch automatisch den Datensatz an die nationale technische Zentraleinheit des Schengener Informationssystems beim Bundeskriminalamt (N.SIS). Diese leitet die Daten an den Zentralrechner des Schengener Informationssystems (C.SIS) in Straßburg und die anderen N.SIS elektronisch weiter. Da die nationalen Datenbestände (INPOL) von den Schengen-Datenbeständen getrennt geführt werden, sind auch bei einer Auskunft zwei Abfrageschritte erforderlich.

1.1 Die Ausschreibungen zur verdeckten Registrierung im Staatsschutzbereich

In den überprüften Anordnungen bzw. Anträgen zur polizeilichen Beobachtung aus dem Staatsschutzbereich („PB-07-Maßnahmen“) wurde nicht hinsichtlich der unterschiedlichen Anforderungen nach nationalem und europäischem Recht differenziert; die Anordnungen stützen sich formal und inhaltlich lediglich auf § 25 PolG. Die Ausschreibung im Schengener Informationssystem erfolgte (nur) durch das zusätzliche Ankreuzen des entsprechenden Feldes auf dem hierfür vorgesehenen Formular, ohne dass dies in der Anordnung selbst oder in deren Begründung zum Ausdruck kam. Dass die Schengen-Ausschreibung höhere Anforderungen stellt, wurde offenbar übersehen. Dies war ein nicht unerheblicher formaler und inhaltlicher Verstoß. Wir haben das Landeskriminalamt daher gebeten, die Anordnungen zur polizeilichen Beobachtung im Staatsschutzbereich (PB 07) möglichst umgehend daraufhin zu überprüfen, ob außer den Voraussetzungen nach § 25 Abs. 1 PolG (Straftaten mit erheblicher Bedeutung) zusätzlich die höheren Voraussetzungen nach Artikel 99 Abs. 2 SDÜ (außergewöhnlich schwere Straftaten, gegebenenfalls außerdem im erheblichen Umfang) gegeben sind. In der Begründung der Anordnung sollten die Voraussetzungen nach Artikel 99 SDÜ, also nicht nur die nach § 25 PolG, explizit benannt und deren Vorliegen substantiiert dargelegt werden.

In etlichen der geprüften Fälle war nach den Anordnungen bzw. Antragsbegründungen überdies zweifelhaft, ob die Voraussetzungen von Artikel 99 Abs. 2 SDÜ vorlagen. Der verständliche Wunsch, auch einzelne Erkenntnisse darüber zu erlangen, mit wem sich der Betroffene trifft und wo er unterwegs ist, um auf diese Weise ein Bewegungsbild zu erstellen und – ähnlich wie der Verfassungsschutz – vernetzte Strukturen extremistischer Gruppierungen zu erkennen, kann für die Polizei nicht die auf konkrete Anhaltspunkte gestützte Prognose ersetzen, ob der Betroffene voraussichtlich – gegebenenfalls sogar in erheblichem Umfang – außergewöhnlich schwere Straftaten begehen wird. Hier scheint eine gewisse Überlappung mit der Tätigkeit des Verfassungsschutzes vorzuliegen, weil (auch) das Hauptaugenmerk des polizeilichen Staatsschutzes offenbar darauf gerichtet ist, extremistische Strukturen – insbesondere unter Verwendung verdeckter Methoden – noch weit im Vorfeld von konkreten, strafrechtlich relevanten und auf bestimmte Personen beziehbaren Gefahren aufzuhellen. Diese Aufgabe der Informationsgewinnung über verfassungsfeindliche Strukturen hat der Gesetzgeber indessen, vor allem soweit nachrichtendienstliche Mittel zum Einsatz kommen, dem Verfassungsschutz zugewiesen (vgl. z. B. § 3 Abs. 2 des Landesverfassungsschutzgesetzes).

Soweit die Polizei verdeckte Methoden anwendet, darf sie nicht ihren gesetzlichen Auftrag zur Abwehr konkreter Gefahren und zur vorbeugenden Bekämpfung bestimmter Straftaten – im Fall der Ausschreibungen zur verdeckten Registrierung in allen Schengen-Staaten eben „außergewöhnlich schwerer Straftaten“ – aus dem Auge verlieren. Dass dieses Risiko in der Vergangenheit bestanden hat, wird an einigen Fällen aus dem Bereich Rechtsextremismus deutlich: Hier hatten die Betroffenen zum Beispiel in der Vergangenheit an mehreren Skinhead-Konzerten oder anderen Aktivitäten der Skinhead-Szene teilgenommen, ohne dass es zu „außergewöhnlich schweren Straftaten“ im Sinne von Artikel 99 SDÜ gekommen war. Teilweise lagen Straftaten aus dem Bereich der mittleren Kriminalität schon mehr als fünf Jahre zurück und die Antreffensmeldungen deuteten nicht auf neue außergewöhnlich schwere Straftaten hin. Etliche Antreffensmeldungen bezogen sich auch auf die (legale) Teilnahme an Versammlungen extremistischer Organisationen. In einem Fall wurde über eine bereits seit fast zehn Jahren beobachtete Zielperson – sie sei hier A genannt – regelmäßig registriert, dass sie zum Beispiel auf dem Landesparteitag einer nicht verbotenen Partei einen Infostand betrieb oder an Weihnachts- oder Sonnenwendfeiern extremistischer Gruppierungen teilnahm. Das sind typische Informationen, die der Verfassungsschutz über Extremisten gewinnen und auswerten soll. In einem anderen Fall (B) wurde die dritte Verlängerung

einer Ausschreibung zur polizeilichen Beobachtung um ein weiteres Jahr im März 2006 lediglich damit begründet, dass die betreffende Person nach wie vor zur „Kameradschaft X“ gehöre und sich aus den Kontrollmitteilungen die häufige Teilnahme an Skinhead-Konzerten und ähnlichen Treffen ergeben habe. Die Ausschreibung zur polizeilichen Beobachtung erfolgte dann ohne weitere Unterscheidung nicht nur in INPOL-Z bzw. POLAS-BW, sondern auch im Schengener Informationssystem.

Die Voraussetzungen für eine Ausschreibung nach Artikel 99 SDÜ dürften im Staatsschutzbereich in erster Linie bei den sog. Gefährdern vorliegen. Nach einer vom Landeskriminalamt vorgelegten, bundesweit geltenden Definition aus dem Jahr 2004 handelt es sich bei einem „Gefährder“ um eine Person, „zu der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere im Sinne des § 100 a StPO begehen wird“.

Neben der Kategorie des „Gefährders“ wird in der oben genannten Definition aber auch die Kategorie der „relevanten Person“ im Bereich des polizeilichen Staatsschutzes genannt; das ist eine Person, die „Kontakt- oder Begleitperson eines Gefährders, eines Beschuldigten oder eines Verdächtigen einer politisch motivierten Straftat von erheblicher Bedeutung, insbesondere solche im Sinne des § 100 a StPO“, ist. Die vom Landeskriminalamt vorgelegten Anordnungen bezogen sich vielfach auf derartige „relevanten Personen“. Dabei hatte das Landeskriminalamt jedoch übersehen, dass Kontakt- und Begleitpersonen gar nicht mit Maßnahmen nach Artikel 99 SDÜ überzogen werden dürfen. Nach dem Wortlaut des Artikels 99 SDÜ sollen sich Ausschreibungen zur verdeckten Registrierung (nur) auf Personen beziehen, bei denen anzunehmen ist, dass sie selbst außergewöhnlich schwere Straftaten begehen werden. Bei Kontrollmaßnahmen dürfen dann zwar auch Informationen über deren Begleitpersonen erhoben und an die ausschreibende Dienststelle übermittelt werden, die Ausschreibungen dürfen sich aber nicht gezielt auf derartige Begleitpersonen beziehen. Wir haben dem Landeskriminalamt empfohlen, die bisherigen Ausschreibungen im Staatsschutzbereich nach Artikel 99 SDÜ kritisch zu überprüfen und sie, sofern die betreffenden Personen nicht selbst im Verdacht stehen, außergewöhnlich schwere Straftaten zu begehen, sondern nur Kontakt zu solchen Personen haben, im Zweifelsfall zu beenden.

1.2 Ausschreibungen zur verdeckten Registrierung in anderen Deliktsbereichen

Bei den überprüften Anordnungen aus anderen Deliktsbereichen sah es hinsichtlich der inhaltlichen Begründung nicht viel besser aus. Soweit feststellbar, wurden auch diese Anordnungen inhaltlich weitgehend nur auf § 25 Abs. 1 PolG gestützt. Zwar wurde in den Anordnungen ergänzend ausgeführt, dass „eine Ausschreibung nach Artikel 99 SDÜ genehmigt“ wird; in der Begründung wurde hierzu dann aber – offenkundig mit stets gleich bleibender Formulierung – nur ausgeführt, dass die Ausschreibung nach § 25 PolG zur vorbeugenden Bekämpfung des jeweiligen Delikts erforderlich und angesichts der Schwere der zu erwartenden Straftaten verhältnismäßig sei und dass „aus den gleichen Gründen die Ausschreibung zur verdeckten Registrierung nach Artikel 99 (2) SDÜ zulässig“ sei. Aus dieser Formulierung wird deutlich, dass bei der jeweiligen Anordnung nicht nach § 25 PolG und Artikel 99 SDÜ unterschieden wurde, sondern dass der Anordnende offenbar davon ausging, dass die Voraussetzungen nach Artikel 99 Abs. 2 SDÜ bereits dann gegeben sind, wenn die Voraussetzungen des § 25 Abs. 1 PolG vorliegen. Wir haben daher das Landeskriminalamt aufgefordert, auch in den anderen Deliktsbereichen die Anordnungen rasch daraufhin zu überprüfen, ob die strengeren Anforderungen nach Artikel 99 Abs. 2 SDÜ erfüllt sind. Die Tatsache, dass ca. 80 % aller Ausschreibungen zur polizeilichen Beobachtung nicht nur auf nationaler Ebene, sondern zugleich im Schengener Informationssystem verfügt wurden, während dies in Bayern „nur“ bei rund 15 % der Ausschreibungen der Fall war, deutet darauf hin, dass das Landeskriminalamt Baden-Württemberg die Vo-

raussetzungen für die Ausschreibungen in beiden Systemen zu häufig gleichgesetzt hat. Wir haben dem Landeskriminalamt empfohlen, das Prüfraster für die Anordnungen der polizeilichen Beobachtung künftig für alle Deliktsbereiche einheitlich, jedoch deutlich differenziert nach den unterschiedlichen Voraussetzungen für die nationale und die internationale Ebene zu gestalten. In den Begründungen sollte das in Frage stehende Delikt klar benannt werden und mit den Anforderungen nach § 25 Abs. 1 PolG bzw. Artikel 99 Abs. 2 SDÜ abgeglichen werden.

1.3 Die „Altfälle“

Wie gesagt, liefen viele Anordnungen zur verdeckten Registrierung nach Artikel 99 SDÜ schon seit mehreren Jahren und wurden jährlich erneuert, ohne dass ein konkretes strafrechtliches Ermittlungsverfahren wegen einer „außergewöhnlich schweren Straftat“ in Sicht kam, zu dem die angeordnete Maßnahme etwas hätte beitragen können. In einigen Fällen wurde die Verlängerung ausdrücklich damit begründet, dass sich im zurückliegenden Anordnungszeitraum nichts geändert habe und der Betreffende immer noch zur rechts- oder linksextremistischen Szene oder zu einer mutmaßlich islamistischen Organisation gehöre, die es zu beobachten gelte. In manchen Fällen war für den zurückliegenden Anordnungszeitraum überhaupt keine Antreffensmeldung verzeichnet. In einem Fall (C) hatten sich seit der erstmaligen Ausschreibung im Januar 2004 keine neuen Erkenntnisse ergeben; hier hieß es zur Begründung der Verlängerung lediglich, dass sich in Zukunft in den Räumlichkeiten des Y-Vereins erneut Vorfälle wie im November 2003 ereignen könnten (die damals auf die Unterstützung einer ausländischen terroristischen Vereinigung hätten hindeuten können), dass die Maßnahme aber weiter fortgesetzt werden müsse, weil der Betroffene immer noch Funktionär des Vereins sei. In einem anderen Fall (D) lief die polizeiliche Beobachtung schon seit August 2000; hier wurde in der erneuten Verlängerung sogar explizit erklärt, dass „im Laufe des vergangenen Jahres keine PB-07-Erkenntnisse mit Staatsschutzbezug zu ... (es folgte der Name der Person) festgestellt werden konnten“. Die Erforderlichkeit der Maßnahme für den beabsichtigten Zweck war damit nicht ausreichend begründet. Denn wenn im zurückliegenden Anordnungszeitraum der Betroffene gar nicht angetroffen wurde und auch sonst keine neuen Erkenntnisse hinzukamen, dann kann schlechterdings nicht behauptet werden, ausgerechnet diese Maßnahme sei nun unbedingt weiter erforderlich, um die Gefahr außergewöhnlich schwerer Straftaten abzuwenden.

Wir haben das Landeskriminalamt daher aufgefordert, die Anordnungen zur polizeilichen Beobachtung insbesondere bei den „Altfällen“, in denen Jahr für Jahr eine Verlängerung ausgesprochen wurde, ohne dass sich aus der Maßnahme wesentliche neue Erkenntnisse in Richtung auf das in Rede stehende Delikt ergeben haben, unter dem Aspekt der (weiteren) Erforderlichkeit kritisch zu überprüfen. An die Begründung einer Verlängerung sollten dabei gegenüber der erstmaligen Anordnung verschärfte Anforderungen gestellt werden; insbesondere sollte bei einer Verlängerung klar herausgestellt werden, welche neuen und zusätzlichen Erkenntnisse gerade durch die angeordnete polizeiliche Beobachtung im zurückliegenden Jahr gewonnen wurden und in welchem logischen Zusammenhang diese mit der mutmaßlichen außergewöhnlich schweren Straftat stehen, die die Polizei dem Betroffenen zutraut. Wenn der Betroffene über Jahre hinweg entweder gar nicht oder nur in wirklich unverfänglichen Situationen angetroffen wurde (z. B. bei der Fahrt mit Frau und Kindern in den Urlaub), dann ist eine fortgesetzte polizeiliche Beobachtung nicht mehr gerechtfertigt, sondern dann sind – wenn die behauptete Gefahr wirklich drohen sollte – intensivere Maßnahmen der Erkenntnisgewinnung erforderlich. Immerhin handelt es sich bei der heimlichen polizeilichen Beobachtung um einen Grundrechtseingriff, der nur dann zu rechtfertigen ist, wenn er zur Wahrung höherwertigerer Rechtsgüter erforderlich ist. Zwar ist die polizeiliche Beobachtung – anders als die sog. Rasterfahndung – eine Maßnahme, die einen konkreten Verdacht gegen eine bestimmte Person erfordert. Dennoch ist

davon auszugehen, dass die vom Bundesverfassungsgericht in seinem Beschluss vom 4. April 2006, 1 BvR 518/02, angestellten Erwägungen zur Konkretheit einer Gefahr sich zumindest teilweise auf die polizeiliche Beobachtung übertragen lassen. Dementsprechend sollte auch bei den Anordnungen zur polizeilichen Beobachtung verstärkt Wert darauf gelegt werden, dass die Anhaltspunkte, die für die drohende außergewöhnlich schwere Straftat sprechen, hinreichend konkret benannt werden. Wenn sich im Zeitraum der letzten Anordnung keine neuen und weiterführenden Erkenntnisse aus der Beobachtung ergeben haben, dann ist die Maßnahme auch nicht mehr erforderlich und sollte beendet werden.

1.4 Die verdeckte Registrierung von „Gruppen“

Die hohe Anzahl der Anordnungen zur polizeilichen Beobachtung in Baden-Württemberg war in erster Linie darauf zurückzuführen, dass viele Maßnahmen auf einem gemeinsamen Tatzusammenhang beruhten und eine Vielzahl von Personen betrafen. Im Staatsschutzbereich ging es insoweit um Mitglieder oder Funktionäre mutmaßlich extremistischer Organisationen, im Bereich der sonstigen Kriminalität handelte es sich vielfach um Mitglieder von mutmaßlich kriminellen Banden. Wie wir festgestellt haben, wurden in den Anordnungen, die eine Vielzahl von Personen betrafen, jedoch häufig keine „personenscharfen“ Begründungen gegeben, warum gerade die polizeiliche Beobachtung einer bestimmten Person erforderlich sein sollte, d. h. es wurde auf die einzelne Person bezogen keine Gesamtwürdigung begangener Straftaten bzw. keine an Tatsachenfeststellungen orientierte Prognose für die Begehung künftiger Straftaten mit erheblicher Bedeutung (vgl. § 25 Abs. 1 PolG) vorgenommen bzw. dokumentiert. Da inhaltlich nicht auf die strengeren Anforderungen nach Artikel 99 Abs. 2 SDÜ abgehoben wurde, fehlte erst recht eine Prognose für die Begehung außergewöhnlich schwerer Straftaten. Vielmehr bezogen sich Feststellungen und Prognose häufig auf die Gruppe als solche. Hier ist künftig eine weitaus differenziertere und individuellere Begründung erforderlich.

1.5 Wie das Landeskriminalamt reagierte

Weil das Landeskriminalamt schon während unseres Kontrollbesuchs zu erkennen gab, dass es mit dem bisherigen Verfahren zur verdeckten Registrierung bzw. polizeilichen Beobachtung nicht zufrieden war und dieses grundlegend überarbeiten wollte, haben wir von einer förmlichen Beanstandung – die wegen der fehlenden Bezugnahme auf die strengeren Anforderungen nach Artikel 99 SDÜ und der Einbeziehung von Kontakt- und Begleitpersonen eigentlich angebracht gewesen wäre – abgesehen. Das Landeskriminalamt hat inzwischen unsere Bedenken und Anregungen aufgegriffen und einige Verbesserungen vorgenommen:

– Das Landeskriminalamt wird die Ausschreibungen künftig nach der jeweiligen Rechtsgrundlage differenzieren. Es will verstärkt darauf achten, dass in der Anordnung die Voraussetzungen nach Artikel 99 SDÜ explizit benannt und substantiiert begründet werden, insbesondere die Anhaltspunkte, welche für die drohende Gefahr sprechen.

– Das Landeskriminalamt hat sich unserer Rechtsauffassung angeschlossen, dass „relevante Personen“ bzw. „Kontakt- und Begleitpersonen“ nicht im Schengener Informationssystem (übrigens auch nicht – wie die entsprechende Polizeidienstvorschrift klarstellt – im nationalen System nach § 25 PolG) ausgeschrieben werden dürfen. Das Landeskriminalamt hat zugesagt, künftig im Rahmen der Fachaufsicht besonders darauf zu achten, dass entsprechende Personen weder gemäß Artikel 99 SDÜ noch nach § 25 PolG zur polizeilichen Beobachtung ausgeschrieben werden; es will den Dienststellen zeitnah überarbeitete bzw. angepasste einheitliche Antragsformulare zur Verfügung stellen, in denen explizit auf diesen Umstand hingewiesen wird.

– Die Zweckmäßigkeit eines einheitlichen Prüfrasters wird auch vom Landeskriminalamt gesehen. Hierzu hat es ein einheitliches Antrags-

formular für die Dienststellen der Landespolizei sowie ein einheitliches Anordnungsformular für die zuständigen Organisationseinheiten im Landeskriminalamt selbst erstellt. Die Formulare stellen gegenüber den bisher verwendeten Unterlagen eine deutliche Verbesserung dar.

– Das Landeskriminalamt sieht ebenfalls das Erfordernis, bei „Gruppen“ künftig auf differenziertere und individuellere Begründungen zu achten, und hat unsere Anregung bei der inhaltlichen Gestaltung der entsprechenden Formulare aufgegriffen.

Nicht oder nicht ganz ist uns das Landeskriminalamt in anderen Punkten gefolgt:

– Das Landeskriminalamt räumt zwar ein, dass der Begriff der „außergewöhnlich schweren Straftat“, den das deutsche Recht in dieser Form nicht kennt, enger zu sehen ist als der Begriff „Straftaten von erheblicher Bedeutung“. Es will jedoch von einer Prüfung der einzelnen Anordnungen vorerst absehen, weil es mit einer Absenkung der Anforderungen auf europäischer Ebene rechnet. Es hat uns nämlich wissen lassen, dass im Zusammenhang mit der Weiterentwicklung des Schengener Informationssystems (SIS II) beabsichtigt sei, den Begriff der „außergewöhnlich schweren Straftat“ durch den Begriff der „schweren Straftat“ zu ersetzen. Das Landeskriminalamt will daher an seiner bisherigen Praxis und Auslegung des Begriffs für die Ausschreibung nach Art. 99 Abs. 2 SDÜ festhalten. Aus unserer Sicht wäre ein Festhalten an der bisherigen Auslegung nur für eine kurze Übergangszeit vertretbar. Sollte sich die Einführung des Schengener Informationssystem II weiter verzögern – was sich bereits abzeichnet –, dann muss das Landeskriminalamt die notwendige Einzelfallüberprüfung rasch in Angriff nehmen. Es ist nicht hinnehmbar, dass europaweite Ausschreibungen im Polizeicomputer bleiben, für die die rechtlichen Voraussetzungen nicht gegeben sind.

– Hinsichtlich der wiederholten Ausschreibungen teilt das Landeskriminalamt unsere Auffassung nicht, dass eine Ausschreibung zu beenden sei, wenn eine Person während des Anordnungszeitraums überhaupt nicht angetroffen werde. Die Ausschreibung zur polizeilichen Beobachtung diene zwar nur zur Abrundung weiterer Erkenntnisquellen über die betreffende Person, dies spreche aber nicht gegen die Zulässigkeit der Maßnahme. Die polizeiliche Beobachtung nutze die Ergebnisse polizeilicher Personenkontrollen jedweder Art für Fahndungs- und Ermittlungszwecke. Innerhalb eines Jahreszeitraums könne nicht immer zwingend mit Antreffmeldungen gerechnet werden, insbesondere nach Wegfall der Grenzkontrollen in den Schengenstaaten ergäben sich zwangsläufig wesentlich weniger Antreffsituationen und damit einhergehend auch weniger Antreffmeldungen. Unseren Bedenken will das Landeskriminalamt aber dadurch Rechnung tragen, dass in der Regel nur noch eine bis zu dreimalige Verlängerung der Anordnung zulässig sein soll, wobei die Verlängerung auf neue einschlägige Erkenntnisse zu stützen ist. Wenn sich in diesem Zeitraum keine neuen Erkenntnisse ergeben, die die bisherige Bewertung stützen, soll die Ausschreibung grundsätzlich gelöscht werden. Damit lässt sich aus unserer Sicht bis auf weiteres leben. Wir haben vor, die neue Verfahrensweise zu beobachten und gelegentlich erneut zu überprüfen.

Wie sieht die Gesamtbilanz der Ausschreibungen zur polizeilichen Beobachtung bzw. verdeckten Registrierung nunmehr aus? Hierzu teilte uns das Landeskriminalamt mit, dass mit Stand 16. Oktober 2006 noch 315 Personen in den nationalen Systemen und im Schengener Informationssystem ausgeschrieben waren, davon 66 Personen nur in den nationalen Systemen. Von den ursprünglich im Staatsschutzbereich ausgeschriebenen 118 Personen seien mittlerweile 67 gelöscht. Kontakt- oder Begleitpersonen („relevante Personen“) seien nicht mehr ausgeschrieben. Auch in den oben genannten Einzelfällen (A-D) seien die Ausschreibungen gelöscht worden.

## 2. Das Akkreditierungsverfahren im Rahmen der Fußball-Weltmeisterschaft 2006 und die Mitwirkung der Sicherheitsbehörden

Die Fußball-Weltmeisterschaft 2006 war nicht nur ein großer sportlicher und organisatorischer Erfolg für den Deutschen Fußball-Bund (DFB), sie war unstreitig auch eine gewaltige Herausforderung für die deutschen Sicherheitsbehörden. Dies nicht nur wegen der möglichen Auseinandersetzungen zwischen gewalttätigen Hooligans, sondern auch wegen der verbreiteten Sorge vor terroristischen Anschlägen, die zu allen denkbaren Vorkehrungen Anlass gab. Selbst über den Einsatz der Bundeswehr wurde heftig diskutiert und manche kritischen Beobachter sahen im Geiste schon Panzer und Flugabwehrgeschütze vor den Stadien auffahren. Im Rückblick haben sich die Sorgen zum Glück nicht bestätigt. Statt Terrorangst gab es eine überschäumende Begeisterung zahlloser fröhlicher Fußballfans aus aller Welt. Die berechtigte Euphorie und Erleichterung über den friedlichen Verlauf sollte jedoch nicht den Blick dafür trüben, dass aus Sicht des Datenschutzes manches nicht ganz unbedenklich war. Insbesondere wurden bei der Weltmeisterschaft erstmals einige Verfahren und Techniken angewandt, die nicht unbedingt zur Nachahmung empfohlen werden können. Damit meinen wir weniger die Ausstellung personenbezogener Eintrittskarten, auf denen zur besseren Kontrolle die persönlichen Daten des Karteninhabers in einem RFID-Chip enthalten waren – dennoch soll es nach Presseberichten einen florierenden Schwarzmarkt gegeben haben. Wir meinen auch nicht die umfangreiche Videoüberwachung durch die Veranstalter in den Stadien. Mit diesen beiden Aspekten hat sich das Innenministerium als für den Datenschutz im privaten Bereich zuständige Aufsichtsbehörde zu befassen. Uns hat vielmehr die Beteiligung von Polizei und Nachrichtendiensten an dem Akkreditierungsverfahren zur Fußball-WM 2006 beschäftigt.

### 2.1 Das Akkreditierungsverfahren

Veranstalter der Fußball-Weltmeisterschaft 2006 in Deutschland war der Internationale Fußball-Verband (FIFA), ausrichtender Verband der DFB, der zur organisatorischen Bewältigung ein Organisationskomitee einsetzte. Im Rahmen eines umfassenden Sicherheitskonzepts, für das auch die Bundesregierung gegenüber der FIFA gewisse Garantien abgab, wurde frühzeitig beschlossen, Personen, die an den Spieltagen in einer bestimmten Funktion Zutritt zu den Stadien und anderen, vom Veranstalter festgelegten Orten erhalten sollten, im Rahmen eines Akkreditierungsverfahrens einer sog. Zuverlässigkeitsüberprüfung zu unterziehen, um Sicherheitsrisiken auszuschließen. Zu dem davon betroffenen Personenkreis gehörten u. a. Fußballspieler, Mannschaftsbetreuer, Trainer, Funktionäre, Vertreter der Sponsoren, Journalisten und andere Mitarbeiter der Medien, Servicepersonal aller Sparten (z. B. Beschäftigte in der Gastronomie oder Reinigungskräfte), die Mitarbeiter von Hilfsorganisationen, Sanitäts- und Rettungsdiensten, freiwillige Helfer („volunteers“), das Sicherheitspersonal, das von den jeweiligen Stadionbetreibern für die Objektsicherung und Personenkontrollen vorgesehen war, sowie (zunächst) auch die zum Einsatz kommenden Polizeibeamten, die nach unseren Informationen später ausgeklammert wurden und Zutrittsberechtigungen ohne Namen und ohne individuelle Überprüfung erhielten. Das mit den Innenministerien von Bund und Ländern abgestimmte Sicherheitskonzept sah vor, die Daten dieser Personen, deren Zahl zunächst auf bis zu 250 000 geschätzt wurde, mit den bei den Sicherheitsbehörden (Polizeidienststellen, Verfassungsschutzbehörden und Bundesnachrichtendienst) vorhandenen Erkenntnissen abzugleichen. Auf dieser Grundlage sollte das Bundeskriminalamt, bei dem das Verfahren auf Seiten der Sicherheitsbehörden technisch und organisatorisch zusammenlief, ein zusammenfassendes Votum abgeben, das auf eigenen Erkenntnissen und auf den Empfehlungen der weiteren zu beteiligenden Stellen, also auch des Landeskriminalamts Baden-Württemberg und des Landesamts für Verfassungsschutz Baden-Württemberg, beruhte. Die abschließende Entscheidung über die Akkreditierung lag in jedem Fall beim Organisationskomitee. Eingeleitet wurde das Verfahren durch einen Antrag über das Internet beim Organisationskomitee, den freiberuflich Tätige und Selbständige selbst stellen mussten;

bei Arbeitnehmern hatte der jeweilige Arbeitgeber für seine Mitarbeiter Sammelakkreditierungen zu beantragen. Die Betroffenen wurden dabei in einer sog. Datenschutzinformation, die auf der Homepage des Veranstalters abrufbar war, über die mit der Akkreditierung verbundene Verarbeitung personenbezogener Daten, die Überprüfung durch Polizei und Verfassungsschutz sowie über die Ablehnungskriterien informiert. Die mit dem Antrag auf Zulassung verbundene Einwilligungserklärung bezüglich der Verarbeitung ihrer Daten bzw. der Überprüfung hatten Arbeitnehmer gegenüber ihrem Arbeitgeber abzugeben, der diese Einwilligungserklärungen aufzubewahren hatte. Gleichzeitig wurden die Bewerber darauf hingewiesen, dass der Antrag auf Akkreditierung und damit auch die erbetene Angabe persönlicher Daten freiwillig sei, ohne Einwilligung aber keine Akkreditierung erfolgen werde, und dass eine Akkreditierung ohne Angabe von Gründen verweigert werden könne. Das Einverständnis mit der Datenschutzerklärung war elektronisch zu bestätigen.

Auch der interne Abgleich mit den Datenbeständen von Polizei und Verfassungsschutz erfolgte weitgehend automatisiert. Hierzu übermittelte das Organisationskomitee zunächst auf einem Datenblatt elektronisch die zur Durchführung des Verfahrens bestimmten Informationen über die zu akkreditierenden Personen (Grunddaten sowie vorgesehene Funktion). Das Bundeskriminalamt erhielt den Gesamtdatenbestand und prüfte ihn auf „Treffer“ in den dort verfügbaren polizeilichen Informationssystemen ab; die Landeskriminalämter erhielten die Daten über die Personen (mit und ohne „Treffer“), die ihren Wohnsitz in dem jeweiligen Bundesland hatten. Der Bundesnachrichtendienst sollte daneben die Personen mit Auslandsbezug überprüfen. Die Landesämter für Verfassungsschutz, die die Datensätze über das Bundesamt für Verfassungsschutz erhielten, leiteten ihre Empfehlungen über das Bundesamt wieder dem Bundeskriminalamt zu. Dieses teilte das Gesamtvotum ohne vorherige Anhörung des Betroffenen dem Organisationskomitee mit. Sofern sich kein Treffer ergab, erfolgte sofort eine Bestätigung („APPROVED“), fehlerhafte Datensätze (Zusatz „WRONG“) wurden umgehend zur Überprüfung zurückgereicht. Das Organisationskomitee wiederum teilte dann dem Betroffenen – soweit dieser den Antrag selbst gestellt hatte – mit, ob er zugelassen wurde oder nicht. Bei Sammelakkreditierungen wurde nur der Arbeitgeber benachrichtigt.

Warum gab es Einwände gegen dieses Verfahren aus Sicht des Datenschutzes? Die Sicherheits- bzw. Zuverlässigkeitsüberprüfung greift in die Persönlichkeitsrechte der Betroffenen ein. Sie kann zudem in Einzelfällen zu einem Arbeitsplatzverlust oder – soweit es um die Zulassung von Journalisten geht – zu einer Behinderung der Berichterstattung führen und setzt daher eine gesetzliche Grundlage voraus. Eine ausdrückliche gesetzliche Grundlage, wie sie etwa für Sicherheitsüberprüfungen im öffentlichen Dienst oder im Bereich des Luftverkehrs gegeben ist (vgl. z. B. hinsichtlich der Mitwirkung des Landesamts für Verfassungsschutz nach § 3 Abs. 3 des Landesverfassungsschutzgesetzes), besteht für Sportveranstaltungen wie die Fußball-WM allerdings nicht, so dass die Zulässigkeit der Zuverlässigkeitsüberprüfung nur auf die Einwilligung des Betroffenen gestützt werden könnte. Ob bei Maßnahmen im öffentlichen Bereich die Einwilligung des Betroffenen eine gesetzliche Grundlage ersetzen kann, ist zweifelhaft. Wegen des singulären Charakters der Fußball-WM und wegen der abstrakten Gefährdungslage haben wir die Einwilligung des Betroffenen ausnahmsweise als ausreichende Grundlage unter der Voraussetzung angesehen, dass die Zuverlässigkeitsüberprüfung anhand einer eigenen Beurteilung der Sicherheitsbehörden auf das wirklich erforderliche Maß beschränkt wird und die Einwilligung in voller Kenntnis der Prüfungskriterien erfolgt. Diese Anforderungen wurden jedoch nicht vollständig erfüllt. Zum einen wurde die Prüfung auf Personengruppen erstreckt, bei denen eine Überprüfung offenkundig keinen Sinn machte. Zum andern konnten die Betroffenen aufgrund der Datenschutzinformation nicht hinreichend erkennen, unter welchen Voraussetzungen sie abgelehnt werden können. Die Behörden konnten die Prüfung der Erforderlichkeit

auch nicht einfach dem Veranstalter als „Herr des Verfahrens“ überlassen, selbst wenn dieser eine möglichst umfassende Zuverlässigkeitsprüfung wünschte. Auf Einwände der Datenschützer in Bund und Ländern gegen das Verfahren und den weiten Kreis der Betroffenen wurde entgegnet, dass die Zuverlässigkeitsüberprüfung ein „Kernelement der gesamten Sicherheitskonzeption für die WM“ sei, um „die zuständigen Polizeiführer“ in die Lage zu versetzen, „innerhalb kürzester Zeit umfassende Lagebeurteilungen“ durchzuführen. Wir haben allerdings Zweifel, ob das gewählte Verfahren sinnvoll war und ob hier nicht des Guten bei weitem zu viel getan wurde.

Eine Zuverlässigkeitsüberprüfung der von den nationalen Fußballverbänden benannten Delegationsmitglieder (Spieler, Trainer, Masseure, Funktionäre usw.) durch Polizei und Verfassungsschutz war aus unserer Sicht nämlich völlig überzogen und daher auch nicht erforderlich. Was hätte denn eine Überprüfung im Ernstfall ergeben sollen? Entweder hätten die Sicherheitsbehörden keine Erkenntnisse über diesen Personenkreis oder ein wie immer geartetes Überprüfungsergebnis hätte keinen Einfluss auf den Zutritt zu den Stadien haben können. Hätte man zum Beispiel einem Bundesligaprofi, der sich mal wegen einer Trunkenheitsfahrt strafbar gemacht hatte, den Einsatz im Nationaltrikot verweigern wollen? Befürchtete man, ein Funktionär eines ausländischen Fußballverbands könnte ein verkappter Terrorist sein? Was für einen Sinn macht eine Zuverlässigkeitsüberprüfung bei Journalisten, Rettungssanitätern, Feuerwehrleuten und Polizeibeamten? Welches Sicherheitsrisiko soll von dieser Personengruppe ausgehen? Immerhin wurden – angeblich auf Intervention einiger Innenminister – Polizeibeamte schließlich ohne individuelle Zuverlässigkeitsüberprüfung zugelassen. Warum nicht weitere – offenkundig „zuverlässige“ – Personengruppen auf gleiche Weise zugelassen werden konnten, bleibt das Geheimnis der Verantwortlichen. Damit hier kein Missverständnis aufkommt: Es ist völlig unbestritten, dass für eine Großveranstaltung wie die Fußball-WM besondere Zutrittsberechtigungen für die Stadien ausgestellt werden und entsprechende Identitätskontrollen beim Einlass vorgenommen werden müssen. Es wäre auch nichts dagegen einzuwenden, wenn – wie bei Flughäfen – Taschen kontrolliert worden wären. Diese Sicherheitsvorkehrungen sind völlig unbedenklich. Die generelle Überprüfung von Funktionsträgern bei sportlichen oder anderen Großveranstaltungen ist jedoch überzogen und darf nicht zur Nachahmung führen. Und wenn man schon die Platzanweiserin oder den Würstchenverkäufer unter die Lupe nehmen will, dann liegt der Gedanke nicht mehr fern, auch die Zuschauer seien Sicherheitsrisiken und müssten überprüft werden. Hier droht eine unheilvolle Entwicklung. Um es auf den Punkt zu bringen: Es darf nicht so weit kommen, dass man sich eine Eintrittskarte für ein Popkonzert der Rolling Stones oder für ein Formel-1-Rennen nur dann bestellen darf, wenn man sich zunächst damit einverstanden erklärt, dass man von Polizei und Verfassungsschutz überprüft wird. Mit der Sorge vor Terroranschlägen kann zwar viel, aber nicht alles gerechtfertigt werden.

2.2 Die Ablehnungskriterien

In den aus Sicht der Bewerber maßgeblichen Datenschutzinformationen wurde als Ziel der (polizeilichen) Zuverlässigkeitsüberprüfung bezeichnet, einen „sicheren und störungsfreien Verlauf der Veranstaltung“ zu gewährleisten. Es solle verhindert werden, dass „Personen in sicherheitsrelevanten Bereichen tätig werden können, bei denen zu befürchten ist, dass sie eine Gefährdung für die Gesamtveranstaltung darstellen können“. Deshalb werde die Polizei dem Organisationskomitee in folgenden Fällen grundsätzlich und ohne Nennung von Gründen die Ablehnung der Akkreditierung empfehlen:

„ ...

Aus den Dateien ergeben sich rechtskräftige Verurteilungen wegen begangener

– Verbrechen,

– Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie sich gegen das Leben, die Gesundheit oder die Freiheit einer oder mehrerer Personen oder bedeutende fremde Sach- und Vermögenswerte richten, auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- oder Wertzeichenfälschung oder
gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen werden oder

– Staatsschutzdelikte;

– es besteht ein Eintrag in der Datei ‚Gewalttäter Sport'.

..."

Außerdem wurde darauf hingewiesen, dass die Polizei auch bei mehrfacher rechtskräftiger Verurteilung wegen anderer als den oben genannten Delikten mit erheblicher Bedeutung dann eine ablehnende Empfehlung aussprechen werde, wenn dies nach einer sorgfältigen Prüfung aller Umstände angezeigt erscheine. Gleiches gelte, wenn sonstige Erkenntnisse zu der Person des Bewerbers vorlägen, z. B. über laufende oder eingestellte Ermittlungsverfahren oder Strafverfahren ohne gerichtliche Verurteilung, oder wenn Staatsschutz- oder Rauschgifterkenntnisse oder Erkenntnisse aus dem Deliktsbereich Organisierte Kriminalität vorlägen, die darauf schließen ließen, dass der Bewerber künftig solche Straftaten begehen werde.

Aus unserer Sicht waren die Ablehnungsgründe zu weitgehend und zu unbestimmt; es schien unverhältnismäßig, sogar eingestellte strafrechtliche Ermittlungsverfahren oder nicht strafrechtlich relevante Erkenntnisse des Verfassungsschutzes (gegebenenfalls sogar Informationen, die aus geschützten Quellen stammten oder durch G 10-Maßnahmen gewonnen wurden) berücksichtigen zu können. Was bedeutete die „sorgfältige Prüfung aller Umstände" durch die Sicherheitsbehörden? Für die Betroffenen war jedenfalls vorab kaum erkennbar, unter welchen Voraussetzungen sie abgelehnt werden können.

Um festzustellen, wie die Zuverlässigkeitsüberprüfungen in der Praxis durchgeführt und welche Personen nicht zugelassen wurden, haben wir nach Abschluss der Fußball-Weltmeisterschaft die entsprechenden Unterlagen beim Landesamt für Verfassungsschutz und beim Landeskriminalamt näher unter die Lupe genommen.

2.3 Wie das Landesamt für Verfassungsschutz verfuhr

Insgesamt wurde das Landesamt durch das Bundesamt für Verfassungsschutz in 82 Fällen über „Treffer" in der bundesweiten Datei der Verfassungsschutzbehörden (NADIS) unterrichtet und um nähere Überprüfung des Akkreditierungsbewerbers gebeten. In 81 Fällen empfahl das Amt die Zustimmung, in einem Fall eine Ablehnung. 49 Personen waren allerdings nur deswegen in NADIS erfasst, weil sie selbst bereits in anderem Zusammenhang einer Sicherheitsüberprüfung (z. B. als Beamte, die zum Umgang mit Verschlusssachen ermächtigt werden sollten) unterzogen worden waren. Der einzige Ablehnungsfall des Amtes bezog sich auf einen hochrangigen Funktionär der türkischen DHKP-C („Revolutionäre Volksbefreiungspartei-Front"), die eine Nachfolgeorganisation der 1983 vom Bundesminister des Innern verbotenen „Devrimci Sol" darstellt und deshalb 1998 ausdrücklich in das Verbot mit einbezogen wurde. Der betreffende Funktionär war 2004 durch das Oberlandesgericht Frankfurt wegen mitgliedschaftlicher Beteiligung an einer terroristischen Vereinigung (§§ 129 a Abs. 1, Nr. 1 und 3 StGB a. F., § 56 Abs. 1 und 2 StGB) zu einer Freiheitsstrafe von einem Jahr und neun Monaten auf Bewährung verurteilt worden. Eine Ablehnung des auch außerhalb der Landesgrenzen politisch aktiven Bewerbers wurde auch von anderen Verfassungsschutzbehörden empfohlen. Der beim Landesamt für Verfassungsschutz angelegte Vorgang ergab keine Anhaltspunkte für datenschutzrechtliche Verstöße. Eine Beschwerde

des Bewerbers ging weder beim Landesamt für Verfassungsschutz noch bei unserer Dienststelle ein. Die Akten des Ablehnungsfalls werden nach spätestens einem Jahr nach Ende der Fußball-Weltmeisterschaft vernichtet, in den Zustimmungsfällen erfolgte die Vernichtung nach drei Monaten. Dies gilt übrigens auch für die vom Landeskriminalamt bearbeiteten Fälle.

2.4 Was wir beim Landeskriminalamt feststellten

Entgegen den ersten Schätzungen wurden insgesamt bundesweit „nur“ 148 351 Anträge auf Akkreditierung gestellt, davon wurde 144 881 Anträgen zugestimmt, 2 055 Anträge wurden abgelehnt, in 1 331 Fällen war der Datensatz fehlerhaft und 84 Anträge waren noch nicht abschließend bearbeitet. Auf Baden-Württemberg entfielen für den Polizeibereich 10 946 Anträge, von denen 10 670 angenommen und 226 abgelehnt wurden; dies entspricht einer Ablehnungsquote von 2,06 %. In 50 Fällen war der Datensatz fehlerhaft. Hinsichtlich der Zusammensetzung der abgelehnten Bewerber ergab sich eine bemerkenswerte Häufung bei bestimmten Funktionen: 148 Personen (rd. 65,5 % der Ablehnungsfälle) waren als temporäre Mitarbeiter von Sicherheitsfirmen vorgesehen, in 17 Fällen (rd. 7,5 %) handelte es sich um Aushilfskräfte für wechselnde Verwendungen („Springer“), 15 abgelehnte Bewerber (rd. 6,6 %) sollten als Aushilfskräfte im Bewirtungsbereich („Catering“) und acht Personen (rd. 3,5 %) als Aushilfsfahrer eingesetzt werden. Die übrigen 38 abgelehnten Bewerber verteilten sich auf 21 weitere Funktionen. Offenbar hatten ausgerechnet die Sicherheitsfirmen aufgrund des hohen kurzfristigen Personalbedarfs Aushilfskräfte angeworben, die nicht den genannten Zulassungskriterien entsprachen. Nach Mitteilung des Landeskriminalamts baten zehn abgelehnte Bewerber um Auskunft, in 13 Fällen gab es außerdem Gespräche mit den Petenten, in zwei Fällen wurde daraufhin das Votum nachträglich in eine Zustimmung zur Akkreditierung abgeändert. Widerspruchsverfahren oder Klagen gab es nicht. In zwei weiteren Fällen wurden Bewerber, bei denen das Landeskriminalamt zuvor eine Ablehnung empfohlen hatte, vom Veranstalter dennoch zugelassen. Bei unserer Dienststelle gingen keine Beschwerden von abgelehnten Bewerbern ein.

Bei unserem Kontrollbesuch im Landeskriminalamt haben wir uns naturgemäß auf die 226 Ablehnungsfälle konzentriert, aus denen wir nach dem Zufallsprinzip eine Stichprobe von insgesamt 69 Fällen gezogen haben. Die Unterlagen des Landeskriminalamts enthielten neben einem Deckblatt im Wesentlichen ein Datenblatt, aus dem sich weitere personenbezogene Daten des Bewerbers, dessen geplante Funktion bei der Fußball-WM, der Verfahrensstand sowie die Treffer in den verschiedenen polizeilichen Dateien ergaben. Schließlich war den Unterlagen noch ein aktueller Ausdruck aus dem Polizeilichen Auskunftssystem des Landes (POLAS-BW) beigefügt, der auch Hinweise auf Eintragungen im polizeilichen Informationssystem des Bundes und der Länder (Verbundsystem INPOL-Z beim Bundeskriminalamt) und im Schengener Informationssystem enthielt. Zum Ablauf des Verfahrens und zur internen Entscheidungsfindung wurde uns erklärt, dass – soweit die Informationen aus dem polizeilichen Auskunftssystem nicht ausreichend oder interpretierungsbedürftig waren – jeweils eine Stellungnahme der aktenführenden Dienststelle vor Ort eingeholt worden sei. Diese Anfragen waren auch in den vorgelegten Unterlagen vorhanden. Längere Berichte der aktenführenden Dienststelle waren nur vereinzelt, die staatsanwaltschaftlichen oder gerichtlichen Entscheidungen gegen den Betroffenen aus den vorgelegten Unterlagen gar nicht ersichtlich. Offenkundig war in den meisten Ablehnungsfällen der POLAS-Ausdruck maßgeblich und ausreichend gewesen. Viele Kontakte mit den Dienststellen liefen ausweislich der handschriftlichen Notizen auch telefonisch ab, was sich durch den hohen Zeitdruck erklärte. „Grenzfälle“ wurden in der Gruppe der Bearbeiter des LKA durchgesprochen und entschieden.

Zusammenfassend lässt sich konstatieren, dass die vom LKA dokumentierten Gründe für die Ablehnung von Bewerbern im Wesentlichen

nachvollziehbar waren und formal auch den in den Datenschutzinformationen genannten Ablehnungskriterien entsprachen. Dass die bundesweit abgestimmten und einheitlich angewandten Ablehnungskriterien aus unserer Sicht zu streng waren, kann dem mit der Umsetzung befassten LKA nur bedingt angelastet werden. Diese Kritik trifft in erster Linie die Innenministerien von Bund und Ländern, die die Kriterien ausgearbeitet hatten und sich dabei offenkundig von dem Gedanken hatten leiten lassen, alle Risiken auszuschließen und im Zweifel lieber einen Bewerber mehr als einen weniger abzulehnen. Ergebnis dieser Sicherheitsstrategie war u. a., dass in einer Vielzahl der geprüften Fälle die Ablehnung nicht auf rechtskräftige Verurteilungen wegen Verbrechen oder gravierenden Vergehen, die „im Einzelfall nach Art und Schwere geeignet waren, den Rechtsfrieden besonders zu stören", gestützt wurde, sondern dass der in den Kriterien genannte „Auffangtatbestand" Platz griff („wiederholte Tatbegehung ohne gerichtliche Verurteilung unter Würdigung der Gesamterkenntnisse"). Insbesondere die unscharfe „Würdigung der Gesamterkenntnisse" bot dabei naturgemäß einen breiten Spielraum für Interpretationen.

Gemessen an der öffentlich vielfach proklamierten Zielsetzung des Akkreditierungsverfahrens, nämlich die Gefahr von Terroranschlägen in den Stadien durch „Innentäter" zu vermeiden, zeigte die praktische Umsetzung jedenfalls, dass die Zuverlässigkeitsüberprüfung im Ergebnis auch der Abwehr der „Alltagskriminalität" zu dienen hatte. Im Zweifel wurde eher „auf Nummer sicher" gegangen. So war in den Datenschutzinformationen u. a. als Ziel der polizeilichen Zuverlässigkeitsüberprüfung bezeichnet worden, Personen fernzuhalten, die „eine Gefährdung für die Gesamtveranstaltung darstellen" könnten. Der unbefangene Leser wird dabei vermutlich an die berechtigte Sorge der Veranstalter vor mutmaßlichen Terroristen, prügelnden Hooligans oder Neonazis in den Stadien gedacht haben. Dass aber Straftäter aus dem Bereich der mittleren Kriminalität die Gesamtveranstaltung Fußball-WM oder auch nur ein einzelnes Spiel in Gefahr bringen könnten, wird ihm nicht in den Sinn gekommen sein und wohl auch niemand behaupten wollen. Damit soll der mögliche Ansehensverlust für das gastgebende Land bei Straftaten in den Stadien nicht in Abrede gestellt werden. Aber bei einer Reihe von Ablehnungsfällen drängte sich schon die Frage auf, welche Gefahr für die Gesamtveranstaltung denn tatsächlich von dem Bewerber im Kontext seines Einsatzes bei der Fußball-Weltmeisterschaft ausgehen sollte. Dies soll an einigen Beispielen illustriert werden:

– Fall 1: Der 1986 in Stuttgart geborene Bewerber kroatischer Nationalität war als Aushilfskraft bei einer Sicherheitsfirma vorgesehen. Die Ablehnung war entsprechend den Ablehnungskriterien darauf gestützt worden, dass er wegen eines oder mehrerer Vergehen verurteilt worden war, das/die nach Art und Schwere geeignet war(en), den Rechtsfrieden besonders zu stören. Angekreuzt waren hierzu die Felder „Leben, Gesundheit, Freiheit" und „Sach- oder Vermögenswerte". Das Datenblatt des Bewerbers wies Treffer in POLAS und in der Verbunddatei INPOL auf. Der POLAS-Ausdruck und ein den Unterlagen beigefügter Ermittlungsbericht zeigten dann Einzelheiten zu zwei Tatkomplexen: So hatte eine Gruppe junger Leute, darunter der abgelehnte Bewerber, in der Nacht zum Ostersonntag 2005 in Stuttgart-Untertürkheim verschiedene Sachbeschädigungen begangen. Er selbst hatte zugegeben, den Briefkasten an einem Wohnhaus mit einem Feuerwerkskörper in die Luft gesprengt zu haben; außerdem beschuldigte ihn einer aus der Gruppe, er habe zusammen mit einem anderen jungen Mann einen Fotofix-Automaten im Bahnhofsgebäude umgeworfen (Sachschaden: 3.000 €). Das Strafverfahren war zum Zeitpunkt der Überprüfung noch nicht abgeschlossen. Der andere Tatkomplex betraf eine Verurteilung wegen Raubes/räuberischer Erpressung im September 2005. Der Bewerber hatte von zwei anderen Heranwachsenden, die er auf der Straße traf, Zigaretten gefordert und sie dann geschlagen und getreten, als sie erklärten, sie hätten keine dabei. Wegen dieses Delikts war der Bewerber vom Amtsgericht

Heilbronn zu 50 Stunden gemeinnütziger Arbeit und einem sozialen Trainingskurs verurteilt worden. Auf dem Bearbeitungsbogen war zu dem Bewerber notiert worden: „Ablehnung gemäß Kriterienkatalog (Tathergang zeugt von erheblichem Gewaltpotenzial, hohe Verurteilung)“.

– Fall 2: Die 1985 geborene Bewerberin war ebenfalls als Aushilfskraft für eine Sicherheitsfirma vorgesehen. Bei ihr wurde die Ablehnung auf das „Auffangkriterium“ („wiederholte Tatbegehung ohne gerichtliche Verurteilung unter Würdigung der Gesamterkenntnisse“) gestützt. Die Bewerberin war mit insgesamt elf Einträgen in POLAS erfasst, darunter mehrere Fälle von Beförderungserschleichungen und Beleidigungen, bei denen das Strafverfahren eingestellt worden oder der Verfahrensausgang nicht bekannt war. Gravierender war eine Verurteilung zu zwei Wochen Jugendarrest im Jahre 2004 durch das Amtsgericht Stuttgart-Bad Cannstatt, weil die Bewerberin im Jahr 2004 zwei im Hof spielende Nachbarskinder bedroht hatte, sie umzubringen, und auch die Mutter der Kinder grob beleidigt hatte. Vorangegangen war eine weitere Verurteilung der Bewerberin zu gemeinnütziger Arbeit wegen Beförderungserschleichung im Jahre 2002. Der handschriftlichen Notiz auf dem Bearbeitungsbogen war nur zu entnehmen, dass es vor der ablehnenden Entscheidung eine interne Diskussion gegeben hatte.

– Fall 3: Der 42-jährige französische Staatsbürger sollte ebenfalls als Aushilfskraft im Sicherheitsbereich eingesetzt werden. Als Ablehnungsgrund war auf dem Deckblatt eine Verurteilung wegen eines oder mehrerer gravierender Vergehen im Bereich „Sach- und Vermögenswerte“ vermerkt. In POLAS war er zuletzt mit zwei Fällen der Beförderungserschleichung im Jahr 2004 erfasst; in dem einem Fall war das Verfahren eingestellt worden, in dem anderen Fall gab es eine Verurteilung zu einer Geldstrafe von 25 Tagessätzen à 20 €. Außerdem war der Bewerber wegen mehrfachen Einmietbetrugs im Jahr 2003 zu einer mehrmonatigen Freiheitsstrafe auf Bewährung verurteilt worden; aus dem Jahr 2002 stammten Verurteilungen zu Geldstrafen wegen falscher uneidlicher Aussage und wegen Sozialleistungsbetrug. Der Bearbeitungsbogen verwies lediglich auf den POLAS-Ausdruck und eine inhaltlich nicht weiter dokumentierte interne Diskussion.

– Fall 4: Der 1980 geborene Stuttgarter wollte als Aushilfskraft im Bereich Catering arbeiten. Im Polizeicomputer war er jedoch als „BTM-Konsument“ – darunter laut einer Randnotiz auch harte Drogen – mit insgesamt sechs strafrechtlich relevanten Vorkommnissen seit dem Jahr 2000 gespeichert. Die Strafverfahren waren jedoch alle eingestellt worden. Darum kam lediglich das „Auffangkriterium“ (s. o.) in Betracht; der Akkreditierungsbewerber wurde abgelehnt. Eine auf den Einzelfall bezogene Begründung, die die strafrechtlichen Ermittlungsverfahren in Relation zu dem beabsichtigten Einsatzzweck setzte, war den Unterlagen nicht zu entnehmen.

– Fall 5: Schließlich verdient auch ein weiterer Fall Erwähnung, bei dem das Landeskriminalamt die Ablehnung der Akkreditierung eines bundesweit bekannten Popsängers empfahl, der – wie auch der Presse bereits zu entnehmen war – wegen Drogendelikten mehrfach mit dem Gesetz in Konflikt geraten war. Der Bewerber war auf dem Datenblatt für die Funktion „Mitarbeiter Sendeanstalt“ vorgesehen, was auf einen Auftritt des Künstlers im Rahmen einer Fernsehsendung bei der Fußball-WM hindeutete.

Bei den oben geschilderten Fällen handelte es sich sicher um Grenzfälle, wie auch der Umstand zeigt, dass es jeweils interne Diskussionen gab, ob die Ablehnungskriterien erfüllt waren oder nicht. Formal kann sich das Landeskriminalamt zur Rechtfertigung darauf berufen, dass in der Datenschutzinformation angekündigt worden war, eine ablehnende Empfehlung ohne weitere Begründung auch auszusprechen, wenn „sonstige Erkenntnisse“ über die Person des Bewerbers, z. B. über laufende oder eingestellte Ermittlungsverfahren oder Strafverfahren, vorliegen.

Dennoch erscheint es in den geschilderten Fällen nahezu unwahrscheinlich, dass die Bewerber im Rahmen der WM erneut einschlägige Straftaten begangen hätten. Die Sicherheitskräfte in den Fällen Nr. 1 und 2 hätten wohl kaum unter den Augen ihres Chefs oder ihrer Kollegen eine Schlägerei mit den Zuschauern angefangen; die Zuschauer hätten wohl auch nicht befürchten müssen, Opfer eines Betrugs durch die Aushilfskraft im Fall Nr. 3 zu werden. Ob der verhinderte Aushilfskellner im Fall Nr. 4 Haschisch oder härtere Drogen in die Stadionwurst gemischt hätte, ist ebenfalls anzuzweifeln. Und dass der abgelehnte Künstler im Fall Nr. 5 einen Fernsehauftritt unter dem Einfluss von Drogen plante, kann auch nicht ohne weiteres angenommen werden.

2.5 Gesamtbewertung

- Erfreulich ist, dass insgesamt nur ein geringer Prozentsatz der Akkreditierungsbewerber (2,06 %) abgelehnt wurde.
- Bei der Akkreditierung hat es sich um ein Massenverfahren gehandelt, das den beteiligten Dienststellen Entscheidungen unter hohem Zeitdruck abgefordert hat. Damit war zwangsläufig eine gewisse Schematisierung mit allen negativen Begleiterscheinungen verbunden. Das Bemühen, jedem einzelnen Fall gerecht zu werden, war zwar unverkennbar, eine bessere Dokumentation des Entscheidungsprozesses hätte dem Verfahren aber gut angestanden. Der in den Verfahrensakten enthaltene POLAS-Ausdruck allein konnte dies nicht leisten.
- Die Ablehnung der Akkreditierung muss – soweit öffentliche Stellen beteiligt sind – geeignet und verhältnismäßig sein. Es wäre daher zu begrüßen gewesen, wenn der Zusammenhang zwischen den Sicherheitsbedenken und der jeweils vorgesehenen Funktion des Bewerbers im Einzelfall deutlicher herausgearbeitet und in der Entscheidungsbegründung festgehalten worden wäre. Bei den Fällen der Stichprobe war die jeweilige Ablehnung nur rudimentär begründet worden. Vertiefte Darlegungen gab es ausweislich der Akten des Landeskriminalamts immerhin bei Nachfragen oder Beschwerden der Betroffenen. Dem Landesamt für Verfassungsschutz, das natürlich wesentlich weniger betroffen war, muss man das Kompliment machen, dass seine (einzige) ablehnende Entscheidung in einem mehrseitigen Vermerk begründet und durch ein angeschlossenes rechtskräftiges Strafurteil gegen den Bewerber unterfüttert worden war.
- Die Ablehnungskriterien haben der Polizei erlaubt, die Ablehnung auch auf polizeiliche Datenspeicherungen wegen Vergehen aus dem Bereich der mittleren Kriminalität zu stützen, bei denen keine rechtskräftigen Verurteilungen vorlagen, sondern die Strafverfahren aus unterschiedlichen Gründen eingestellt worden waren. Damit haben die polizeilichen Datenspeicherungen im Akkreditierungsverfahren eine Bedeutung erlangt, wie sie mit der Speicherung rechtskräftiger Verurteilungen im Bundeszentralregister verbunden ist. Dies ist aber ein grundsätzliches Problem des Verfahrens und der Ablehnungskriterien und weniger dem Landeskriminalamt anzulasten gewesen.
- Ungeachtet der unzureichenden Begründung der Ablehnung in den überprüften Fällen ist andererseits aber auch festzuhalten, dass in der Mehrzahl der Fälle die Sicherheitsbedenken völlig zu Recht erhoben wurden. Die Vorstrafenregister vieler Bewerber waren beachtlich. Bei einigen Bewerbern gab es jeweils mehr als 100 gespeicherte Erkenntnisse in den polizeilichen Dateien. Angesichts dieser Feststellungen drängt sich die Frage auf, wie es überhaupt zu einer Bewerbung gekommen war. In vielen Fällen wäre vermutlich gar kein Akkreditierungsantrag gestellt worden, wenn sich die Arbeitgeber zuvor ein Führungszeugnis ihres für die WM angeworbenen Aushilfsmitarbeiters hätten vorlegen lassen. Den „Vogel abgeschossen“ in dieser Hinsicht hatte bei unserer Stichprobe ein Bewerber, der als Aushilfskraft für den sog. Hospitality-Bereich vorgesehen war, wo vermutlich besondere Freundlichkeit gegenüber den Mitmenschen gefordert war. Ein Einsatz dieses Bewerbers war aber schon deswegen nicht

möglich, weil er zum Zeitpunkt der Überprüfung noch in Untersuchungshaft wegen des Verdachts einer Beteiligung an einem versuchten Totschlag saß. Den Verfahrensakten war außerdem zu entnehmen, dass der Kandidat mehrfach wegen Waffendelikten vorbestraft war und einer berüchtigten Rockergruppe angehörte. Die ablehnende Empfehlung des Landeskriminalamts war hier unvermeidlich und völlig in Ordnung.

### 3. Der Pilotversuch zum Einsatz von „Automatischen Kennzeichenlesesystemen“ (AKLS) in Baden-Württemberg

Bereits seit einigen Jahren befasst sich die Polizei in verschiedenen Bundesländern mit dem Einsatz von – zumeist stationären – Geräten, die die Kennzeichen vorbeifahrender Kraftfahrzeuge erfassen und mit den polizeilichen Fahndungsdateien abgleichen sollen. Im Frühjahr 2004 hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu Bedenken geäußert, u. a. weil es für die verdachtslose Erfassung aller Verkehrsteilnehmer keine gesetzliche Grundlage gab und weil die Gefahr einer ausufernden Nutzung der neuen Technik gesehen wurde (vgl. 25. Tätigkeitsbericht, LT-Drucksache 13/2650). Auf Anfrage ließ uns das Innenministerium damals wissen, dass wegen der offenen rechtlichen Fragen und der schwierigen finanziellen Rahmenbedingungen zurzeit nicht beabsichtigt sei, automatische Kennzeichenlesesysteme einzuführen. 2005 erfuhren wir, dass im Jahr 2006 gegebenenfalls ein Pilotprojekt für den Einsatz von AKLS durchgeführt werde. Die Bestätigung für diese Ankündigung erhielten wir im März 2006, als uns das Landeskriminalamt einen entsprechenden Projektantrag an das Innenministerium mit der Bitte um Prüfung zuleitete.

#### 3.1 Was geplant war

Im Unterschied zu bereits eingeführten stationären Anlagen in anderen Bundesländern sollten die Geräte in Baden-Württemberg testweise zunächst mobil, d. h. bei vier Streifenfahrzeugen der Autobahnpolizeireviere Stuttgart, Weinsberg, Walldorf und Umkirch eingesetzt werden. Die AKLS sollten mit Hilfe von einer oder mehreren Kameras, die fest am Streifenwagen montiert sind (z. B. verdeckt in der Sondersignalleiste auf dem Fahrzeugdach), die Kennzeichen fahrender oder parkender Fahrzeuge erfassen und diese mit dem Sachfahndungsbestand in INPOL abgleichen, wobei die Fahndungsliste auf einer wöchentlich zu aktualisierenden CD-ROM im Fahrzeug mitgeführt wird. Die Erfassung und der Abgleich mit dem Fahndungsbestand sollten vollautomatisch ohne weiteres Zutun der Fahrzeugbesatzung erfolgen. Ergibt der Abgleich eine Übereinstimmung eines erfassten Fahrzeugkennzeichens mit dem Fahndungsbestand („Treffer“), erfolgt ein optischer und akustischer Hinweis; die Besatzung des Streifenwagens sollte dann eine Anfrage bei der Datenstation durchführen, bei Bestätigung des Treffers das Fahrzeug kontrollieren und etwaige Folgemaßnahmen einleiten. Bei Treffern wären das Kennzeichen und das Fahrzeug (ohne Fahrer) von dem System als Bild bis zum Abschluss der polizeilichen Maßnahmen gespeichert worden; eine Speicherung nicht-relevanter Kennzeichen bzw. Fahrzeuge war nicht beabsichtigt. Das AKLS sollte vorrangig auf Verkehrswegen, die für die grenzüberschreitende Kriminalität von Bedeutung sind, d. h. den Bundesautobahnen, zum Einsatz kommen und deshalb dort auch versuchsweise von den vier Autobahnpolizeirevieren getestet werden. Als rechtliche Grundlage des Versuchs wurde § 26 Abs. 1 Nr. 6 des Polizeigesetzes (PolG) angeführt, da der automatisierte Kennzeichenabgleich gegenüber der dort geregelten Personenfeststellung zur Bekämpfung der grenzüberschreitenden Kriminalität („Schleierfahndung“) ein milderes Mittel und daher von der genannten Befugnisnorm mit umfasst sei.

#### 3.2 Was aus Sicht des Datenschutzes zu bemerken war

Bei den Kennzeichen von Kraftfahrzeugen handelt es sich um personenbezogene Daten, weil Kennzeichen einem bestimmten Fahrzeughalter zugeordnet werden können und damit Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten Person liefern

können, vgl. § 3 Abs. 1 LDSG. Automatisierte Kennzeichenlesesysteme sind als technische Mittel zur Anfertigung von Bildaufnahmen und -aufzeichnungen und damit als besondere Mittel der (automatisierten) Datenerhebung und -speicherung im Sinne von § 3 Abs. 2 und 8 LDSG anzusehen. Der Einsatz solcher Systeme stellt daher einen Eingriff in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes dar und bedarf somit einer gesetzlichen – nach dem Projektantrag: polizeirechtlichen – Grundlage. Wegen der für den Einsatz der AKLS geplanten Rahmenbedingungen kamen die Vorschriften über die Videoüberwachung an Kriminalitätsbrennpunkten (§ 21 Abs. 3 in Verbindung mit § 26 Abs. 1 Nr. 2 PolG) als Rechtsgrundlage nicht in Betracht. Ebenso schied ein Rückgriff auf die polizeirechtliche Generalklausel zur Datenerhebung für Zwecke der Gefahrenabwehr oder Störungsbeseitigung (§ 20 Abs. 2 PolG) schon in Ermangelung einer konkreten Gefahrensituation aus; Ziel des anlassunabhängigen Einsatzes von AKLS sollte ja gerade die Erfassung aller Fahrzeuge sein, die das Streifenfahrzeug passiert oder die es passieren. Der anlassunabhängige Einsatz von AKLS konnte auch nicht als Einrichtung einer Kontrollstelle im Sinne von § 26 Abs. 1 Nr. 4 PolG interpretiert werden.

Im Unterschied zum LKA haben wir auch in § 26 Abs. 1 Nr. 6 PolG keine ausreichende Rechtsgrundlage gesehen. Diese Norm gibt der Polizei zwar umfassende Befugnisse für eine verdachtsunabhängige Identitätsfeststellung. Der Einsatz von automatischen Kennzeichenlesesystemen hat jedoch eine andere rechtliche Qualität. § 26 Abs. 1 Nr. 6 PolG betrifft vorrangig individuelle Personenkontrollen, bei denen die Überprüfung der Fahrzeugpapiere und die hiermit verbundene Erhebung von Informationen über Kfz-Kennzeichen und -Halterdaten möglich, aber nicht in allen Fällen zwingend erforderlich ist. Demgegenüber zielt der automatisierte Kfz-Kennzeichenabgleich (zunächst) allein auf das Kfz-Kennzeichen. Außerdem ermöglicht der automatisierte Kfz-Kennzeichenabgleich eine lückenlose Überprüfung aller Fahrzeuge. Die in § 26 Abs. 1 Nr. 6 PolG geregelte „Schleierfahndung“ beschränkt sich zwangsläufig auf Stichproben, weil die Polizei wegen einer Identitätskontrolle von Fahrzeuginsassen ohne konkreten Anlass nicht den gesamten Autobahnverkehr zum Erliegen bringen kann. Der Gesetzgeber ist bei dieser Norm nämlich davon ausgegangen, dass die Polizei Identitätskontrollen nicht unterschiedslos an allen Fahrzeugen bzw. Fahrzeuginsassen durchführt, sondern auf der Grundlage ihres Erfahrungswissens nur stichprobenweise bei solchen, bei denen tatsächliche Anhaltspunkte eine Kontrolle geboten erscheinen lassen.

Auch der nach § 39 Abs. 1 Satz 3 PolG mögliche Abgleich personenbezogener Daten mit dem Fahndungsbestand setzt voraus, dass die fraglichen Daten „im Rahmen der polizeilichen Aufgabenerfüllung“ erlangt worden sind, also bereits aufgrund einer anderen Rechtsgrundlage erhoben wurden. Dies spricht dafür, dass die Daten ohne eine spezifische Rechtsgrundlage nicht allein zum Zweck des Datenabgleichs erhoben werden dürfen. Diese Ansicht wird offenbar auch in anderen Bundesländern vertreten. Anders wäre es kaum zu erklären, dass zum Beispiel das Hessische Gesetz über die Sicherheit und Ordnung und das Bayerische Polizeiaufgabengesetz entsprechend ergänzt wurden, obwohl dort bereits Regelungen für anlassunabhängige Identitätskontrollen enthalten waren. Der seinerzeitige bayerische Regierungsentwurf hatte hierzu klargestellt, dass sich „der Rückgriff auf die Vorschrift ... über die viel umfassendere Identitätsfeststellung ... wegen der andersartigen Eingriffsqualität und Zielrichtung des automatisierten Kennzeichenabgleichs sowie des für Eingriffe in das Recht auf informationelle Selbstbestimmung im Besonderen geltenden Gebots der Normenklarheit als unzureichend“ erweise. Eine gesetzliche Grundlage für den Einsatz von AKLS durch die baden-württembergische Polizei ist daher erforderlich. Dies gilt auch bereits für den beabsichtigten Pilotversuch, da dieser auf die Erhebung und den Abgleich der Kfz-Kennzeichen, also personenbezogener Daten, einer Vielzahl völlig unbeteiligter und unbescholtener

Kfz-Halter unter Echtbedingungen ausgerichtet sein sollte. Bei dem Pilotversuch hätte es sich daher um eine allenfalls zeitlich und räumlich sowie hinsichtlich der Anzahl der Betroffenen geringere, von der rechtlichen Qualität des Eingriffs her jedoch gleichwertige Maßnahme im Vergleich zu dem später beabsichtigten Dauerbetrieb gehandelt. Daher war bereits für den pilothaften Echtbetrieb eine ausreichende Rechtsgrundlage erforderlich. Soweit es um einen rein technischen Funktionstest der in die engere Wahl gezogenen Geräte gegangen wäre, wären Versuchsanordnungen auch ohne die Erhebung von Daten unbeteiligter Dritter denkbar gewesen (z. B. Versuch mit Polizeifahrzeugen, Versuch mit Einwilligung des jeweiligen Fahrzeughalters usw.). Ein derartiger Funktionstest wäre datenschutzrechtlich unbedenklich gewesen.

3.3 Was die Zukunft bringt

Das Landeskriminalamt hat sich seit unserer Stellungnahme nicht mehr gemeldet. Dem Vernehmen nach soll in der durch den Innenminister bereits angekündigten Novelle des Polizeigesetzes aber eine Vorschrift enthalten sein, die den Einsatz automatischer Kennzeichenlesesysteme durch die baden-württembergische Polizei ermöglichen soll. Wir wagen die Prognose: Wenn die neuen Geräte erst mal an den Streifenfahrzeugen der Polizei oder am Straßenrand montiert sind, dann wird es bald nicht mehr nur um die Suche nach gestohlenen Kraftfahrzeugen oder straffälligen Fahrzeughaltern gehen. Über kurz oder lang wird die Verhütung terroristischer Anschläge ins Feld geführt und die Notwendigkeit betont werden, von verdächtigen Personen umfassende Bewegungsprofile anzulegen. Auf Einwände wird dann zu hören sein, es wäre doch schade, eine vorhandene Technik nicht zu nutzen. Die aktuelle Diskussion um die Verwendung der Mautdaten zeigt bereits, wohin die Reise geht.

Was die heutige Realität angeht, so war neulich in der „ADAC-Motorwelt“ zu lesen, dass in den Bundesländern Bayern, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern und Rheinland-Pfalz das polizeiliche „Videoscanning“ bereits eifrig praktiziert werde. Nach dem Bericht soll die Polizei allein in Bayern jeden Monat auf Autobahnen und Bundesstraßen fünf Millionen Nummernschilder scannen. Der ADAC sieht hier eine „neue Dimension der Massenüberwachung“ – dieser Meinung können wir uns nur anschließen.

## 4. Die Überarbeitung der Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK)

Im letzten Tätigkeitsbericht haben wir grundsätzliche datenschutzrechtliche Mängel der Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK) aufgezeigt: Über 40 000 Personen waren in dieser beim Landeskriminalamt (LKA) eingerichteten Datei des Staatsschutzes gespeichert, teilweise ohne Aktenrückhalt oder Nachweis über den zugrunde liegenden Anlass, teilweise ohne Beleg für eine politische Motivation, teilweise viel zu lange, zahlreiche Personen zudem in einer Kategorie („andere Personen“), die in der Errichtungsanordnung für diese Datei gar nicht vorgesehen war (vgl. 26. Tätigkeitsbericht, LT-Drucksache 13/4910). Kurzum: Die Datei musste dringend überarbeitet werden. Nach Veröffentlichung des 26. Tätigkeitsberichts ging eine Stellungnahme des Landeskriminalamts ein, in der erste Abhilfemaßnahmen dargestellt wurden:

– Das LKA schloss sich unserer Auffassung an, dass personenbezogene Daten in einer automatisierten Datei zu löschen sind, wenn ein entsprechender Aktenrückhalt nicht oder nicht mehr vorliegt. Es hat uns mitgeteilt, dass die überprüften Dienststellen die fraglichen Datensätze inzwischen gelöscht hätten. Die übrigen Staatsschutzdienststellen würden noch auf diese Verpflichtung hingewiesen.

– Unsere Forderung, dass auch das der Speicherung zugrunde liegende Ereignis bzw. der Anlass hierfür zu dokumentieren ist, sei von den beteiligten Dienststellen aufgegriffen worden. In Fällen, in denen eine Ergänzung der Datensätze nicht möglich war, seien diese gelöscht worden.

– Das LKA hat bestätigt, dass die Erfassung von Personen in der AD PMK in jedem Einzelfall voraussetze, dass Anhaltspunkte für eine politische Motivation belegt werden können. In den von uns aufgegriffenen Fällen werde nochmals eine sorgfältige Einzelfallprüfung vorgenommen. Soweit sich danach keine Anhaltspunkte ergeben sollten, würden die Datensätze gelöscht.

– Die von uns entdeckten Fälle mit zu langer Speicherfrist seien bereinigt worden. Soweit die Voraussetzungen für eine Fristverlängerung nicht vorlagen, seien die Daten gelöscht worden.

So weit – so gut. Mit unserem Hauptkritikpunkt, dass in der Datei auch „andere Personen“ erfasst worden waren, obwohl diese Gruppe in der Errichtungsanordnung gar nicht vorgesehen ist, hatte das LKA offenbar mehr Probleme. Es ließ uns wissen, dass es unseren Bedenken nur teilweise Rechnung tragen könne. Zunächst sei das Verfahrensverzeichnis entsprechend ergänzt worden. Im Übrigen hielt es das LKA für erforderlich, insbesondere im Zusammenhang mit der Bekämpfung des internationalen Terrorismus auch Personen zu speichern, bei denen nur einzelne Merkmale auf eine Verbindung zum Terrorismus hindeuteten. Zur Begründung verwies das LKA auf die Attentäter von London vom Juli 2005, die aus polizeilicher Sicht unauffällig gelebt hätten, bei denen aber im Nachhinein Indizien für eine zunehmende Radikalisierung erkannt worden seien. Vor diesem Hintergrund sei es notwendig, Indikatoren herauszuarbeiten, die eine hinreichende Beziehung des Betroffenen zur terroristischen Bedrohung herstellen. Es sei u. a. beabsichtigt, Orientierungshilfen in Zusammenarbeit mit den beteiligten Dienststellen zu erarbeiten, um die gespeicherten Personen besser kategorisieren zu können, und insbesondere festzulegen, unter welchen Voraussetzungen jemand als „andere Person“ in der AD PMK gespeichert werden kann. Die zuständigen Dienststellen sollten dann die bestehenden Datensätze anhand dieser Orientierungshilfen überprüfen und gegebenenfalls löschen. Da für die Prüfung jedes Datensatzes durchschnittlich 20 Minuten erforderlich und die Datensätze ungleich auf die Dienststellen verteilt seien, werde die Überprüfung der Datensätze etwa ein halbes Jahr in Anspruch nehmen – gerechnet ab Einführung der Orientierungshilfen.

So erfreulich es war, dass das LKA einige der von uns festgestellten Mängel rasch beseitigt hatte, so schwer wog andererseits der Umstand, dass es im Grunde an der Speicherung der „anderen Personen“ festhalten wollte und zunächst nur die formale Seite bereinigt hatte. Denn wir hatten bereits in unserem 26. Tätigkeitsbericht vorsorglich darauf hingewiesen, dass sich die Unzulässigkeit der polizeilichen Praxis allein durch eine entsprechende Änderung des Verfahrensverzeichnisses bzw. der Errichtungsanordnung nicht beheben ließe. Wir waren daher auf die angekündigten Orientierungshilfen gespannt, die für die Anwendung der AD PMK in der Praxis eine zentrale Rolle spielen sollten.

Im Juni 2006 hat uns das LKA dann einen Entwurf zur Stellungnahme zugeleitet; eher beiläufig ließ es uns wissen, dass sage und schreibe 24 000 Personen in der AD PMK als „andere Person“ gespeichert sind. Danach fallen weit mehr als die Hälfte der in der AD PMK gespeicherten Personen unter diese Kategorie. Offenbar hatten die Staatsschutzdienststellen hier über Jahre hinweg einen willkommenen Auffangtatbestand für alle Datensätze gefunden, die in keine der gängigen polizeirechtlichen „Schubladen“ passten. Die Polizei darf personenbezogene Daten in automatisierten Dateien nämlich nicht nach Gutdünken einspeichern, sondern nur, wenn die Betroffenen bestimmten, in §§ 38, 37 Abs. 1 in Verbindung mit § 20 Abs. 2 bis 5 des Polizeigesetzes (PolG) abschließend genannten Kategorien angehören. Im Wesentlichen muss es sich bei den Betroffenen danach um Straftatverdächtige, potenzielle Straftäter, deren Kontakt- oder Begleitpersonen, potenzielle Opfer, Personen im Umfeld einer gefährdeten Person, Zeugen, Hinweisgeber oder sonstige Auskunftspersonen handeln. Insofern ist es nicht hinzunehmen, dass mehr als die Hälfte der in der AD PMK gespeicherten Personen zu den „anderen Personen“ gehören, denn damit sind nach der Diktion des Polizeigesetzes eigentlich sog. Nichtstörer gemeint, also Personen, die gerade keine Gefahr für die öffentliche Sicherheit oder Ordnung darstellen. Derartige Personen können nach § 20 Abs. 2 PolG nur

zur Abwehr einer (konkreten) Gefahr oder zur Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung gespeichert werden. Der Speicherung „anderer Personen“ in der AD PMK sind nach dem Verhältnismäßigkeitsgrundsatz daher enge Grenzen gesetzt. Schließlich soll es – wie der Dateiname sagt – um politisch motivierte Kriminalität gehen und nicht um das Sammeln von Daten über legales Verhalten. Dem müssen zwangsläufig auch die neuen Orientierungshilfen Rechnung tragen.

Leider ließ der vorgelegte Entwurf keine grundlegende Kursänderung erkennen; das LKA tat sich – wie an den folgenden Beispielen des „potenziellen Straftäters“, der „Kontakt- oder Begleitperson“ und der „anderen Person“ dargestellt werden soll – mit einer rechtlich einwandfreien Abgrenzung des einzuspeichernden Personenkreises nach wie vor schwer:

– Nach § 37 Abs. 1 in Verbindung mit § 20 Abs. 3 Nr. 1 PolG darf die Polizei Daten über potenzielle Straftäter erheben und speichern. Dann müssen aber tatsächliche Anhaltspunkte dafür vorliegen, dass die Betroffenen künftig Straftaten begehen werden; bloße Vermutungen reichen nicht aus. Tatsächliche Anhaltspunkte können sich aus bestimmten Indizien ergeben, aus denen nach polizeilicher Erfahrung auf einen künftigen Geschehensverlauf – in diesem Fall auf eine politisch motivierte Straftat – geschlossen werden kann. Dass dies in der Praxis oft schwierig ist, verkennen wir nicht. Das LKA schreibt in den Orientierungshilfen auch zutreffend, dass die Prüfung der Speicherung eine argumentative und präzise Auseinandersetzung des polizeilichen Sachbearbeiters mit dem fraglichen Anhaltspunkt und der jeweiligen Schlussfolgerung voraussetze und in die Feststellung münden müsse, dass der Anhaltspunkt die Schlussfolgerung trägt. Nicht nachvollziehen konnten wir aber, dass der Anhaltspunkt insbesondere dann die Schlussfolgerung tragen soll, wenn ein Anhaltspunkt aus Sicht eines objektiven Betrachters auch ohne weiteres für ein unverdächtiges Verhalten typisch ist. Wollen wir dem LKA zugute halten, dass es sich nur um einen Schreibfehler gehandelt hat und das Wörtchen „nicht“ gefehlt hat. Die vom LKA genannten Beispiele, aus welchen Anhaltspunkten auf eine drohende politische Straftat geschlossen werden könnte, waren für uns ebenfalls nur teilweise nachvollziehbar. Wenn beispielsweise als Anhaltspunkte „enger Kontakt zu einem radikalen Imam“ oder „tiefgreifende Änderung in der religiösen Auffassung“ genannt sind, dann reichen diese Indizien unter der Überschrift „potenzielle Straftäter“ unseres Erachtens nicht aus; es sollten weitere, strafrechtlich relevante Indikatoren wie etwa Verherrlichung von Gewalt durch den Betroffenen hinzukommen. Bedenklich ist vor diesem Hintergrund auch die Absicht, jemand ohne weiteres als „Funktionär eines Vereins, der dem gewaltbereiten islamistischen Spektrum zuzurechnen ist“ oder sogar als „einfaches Mitglied“ eines solchen Vereins unter die Kategorie „potenzieller Straftäter“ zu fassen. Da ist der Hinweis des LKA nur ein schwacher Trost, dass bei etwaigen „Mitläufern“ auch eine verkürzte Speicherfrist in Betracht komme. Aus unserer Sicht ungeeignet war auch das Beispiel „Häufige Einladung von angeblichen Geschäftspartnern aus dem Ausland plus nicht plausible Angaben“. In den Erläuterungen hierzu wurde auf polizeiliche Erfahrungen verwiesen, wonach radikale Imame oder islamistische Rekrutierer für den „Heiligen Krieg“ unter falschen Angaben eingeladen und dann hier aktiv würden. Die Gastgeber würden auf diese Weise der Fanatisierung und künftigen strafbaren Handlungen Vorschub leisten. Bei allem Verständnis für die schwierige Aufgabe der Terrorismusbekämpfung: Der Bezug zu möglichen Straftaten ist bei diesem Beispiel viel zu vage und der Zusammenhang mit einer politischen Motivation zudem kaum erkennbar, außerdem sind die genannten Verdachtskriterien („angebliche Geschäftspartner“, „nicht plausible Angaben“) nahezu beliebig interpretierbar. Ohne weitere – strafrechtlich wirklich handfeste – Indizien darf der Gastgeber eines Besuchers aus dem Ausland nicht als „potenzieller Straftäter“ in der AD PMK gespeichert werden. „Potenzielle Straftäter“ sah das LKA aber auch außerhalb der Zielgruppe Islamisten: So wollte das LKA Teilnehmer an einem Skinhead-Konzert erfassen, weil dort erfahrungsgemäß neue Angehörige der latent gewaltbereiten Skinhead-Szene rekrutiert würden. Oder aber Besucher von Skinhead-Konzerten sollten dann gespeichert werden,

wenn „bei diesen oder ähnlichen Veranstaltungen“ bekannt werde, dass (andere) Teilnehmer „einschlägige Straftaten“ verübt haben, oder wenn die Planung des Konzerts „unter konspirativen Umständen“ stattfand. Schließlich sollten auch Angehörige der gewaltbereiten Skinhead-Szene generell als „potenzielle Straftäter“ gespeichert werden. So ganz wohl war dem LKA bei diesen Beispielen anscheinend doch nicht, denn es fügte in einer Fußnote hinzu, dass gegebenenfalls „schwächeren Anhaltspunkten“ durch eine verkürzte Speicherfrist Rechnung getragen werden müsse. Hierzu ist zu sagen: Solange die Teilnahme an einem Skinhead-Konzert oder die Zugehörigkeit zur Skinhead-Szene selbst nicht strafbar ist, sind die genannten Kriterien ungeeignet. Wenn der Betroffene selbst eine Straftat begeht, kommt eine Datenspeicherung nach § 38 PolG in Betracht. Solange der Betroffene selbst keine Straftat begeht, kann er auch nicht – vor allem nicht als potenzieller Straftäter – deswegen eingespeichert werden, weil andere bei Skinhead-Konzerten oder innerhalb der Skinhead-Szene erfahrungsgemäß Straftaten begehen. Sofern die Voraussetzungen nicht vorliegen, kann auch eine verkürzte Speicherfrist die Speicherung nicht rechtfertigen.

– Nach § 37 Abs. 1 in Verbindung mit § 20 Abs. 3 Nr. 2 PolG darf die Polizei auch die Daten der „Kontakt- und Begleitpersonen“ von potenziellen Straftätern erfassen und speichern. Zu Recht weist das LKA hier auf eine einschlägige Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2001 hin, wonach der Begriff der Kontakt- und Begleitperson restriktiv auszulegen ist; Voraussetzung sind danach „konkrete Tatsachen für einen objektiven Tatbezug“ und damit für eine „Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten“. Die vom LKA anschließend genannten Beispiele wecken aber Zweifel, ob in der Praxis diesen Anforderungen Rechnung getragen werden wird. So sind nach Ansicht des LKA Kontakt- und Begleitpersonen (und damit gegebenenfalls in der AD PMK zu speichern) die „Mitglieder einer rechtsextremistischen Kameradschaft um die Zielperson A“, die sich regelmäßig zu einem „Kameradschaftsabend“ treffen. Wir meinen dagegen: Wenn aus dem Handeln der Zielperson kein konkreter Straftatenbezug hervorgeht, können anwesende Kontakt- oder Begleitpersonen nicht in Straftaten verwickelt sein, es sei denn, die Teilnahme an der Veranstaltung selbst wäre strafbar oder die Zielperson würde dabei mit Wissen und Wollen der anderen Teilnehmer Straftaten begehen. Die Teilnehmer an einem Treffen einer nicht verbotenen Vereinigung dürfen daher nicht ohne weiteres gespeichert werden. Insofern gibt es vom Gesetzgeber gewollte Unterschiede zwischen den Betätigungsfeldern des polizeilichen Staatsschutzes und des Verfassungsschutzes: Es kann nicht Aufgabe der Polizei sein, personenbezogene Daten von Extremisten ohne Straftatenbezug und ohne eine konkrete Gefahr zu speichern.

– Schließlich müssen die Orientierungshilfen auch dem Umstand Rechnung tragen, dass Personen der Kategorie „andere Person“ nur im absoluten Ausnahmefall eingespeichert werden dürfen (s. o.) und nicht – wie bisher – in der Mehrzahl der Fälle die Grundlage der Datenspeicherung in der AD PMK bilden. Bei der Erhebung und Speicherung von Daten von „anderen Personen“ sind im Hinblick auf die damit verbundene erhebliche Eingriffsintensität, auf die die Orientierungshilfen zutreffend hinweisen, erhöhte Anforderungen zu beachten, die die Rechtsprechung auch in anderem Zusammenhang für die Inanspruchnahme von Nichtstörern aufgestellt hat (vgl. insbesondere BVerfG, Beschluss vom 4. April 2006, 1 BvR 518/02, zur Rasterfahndung). In den Orientierungshilfen wird zwar der Versuch unternommen, die maßgeblichen Gesichtspunkte als Handlungsempfehlung für die bevorstehende Überprüfung des Datenbestandes in der AD PMK durch die Polizeidienststellen zu benennen. Die gewählten Formulierungen lassen jedoch Zweifel aufkommen, ob die erforderliche erhebliche Reduzierung des Datenbestandes von „anderen Personen“ auf diese Weise gelingen kann: Wenn beispielsweise davon die Rede ist, dass die Speicherung „anderer Personen“ in der AD PMK nach den Erfahrungen der polizeilichen Praxis, insbesondere im Zusammenhang mit der Bekämpfung des internationalen Terrorismus, „fachlich

geboten sein kann“ und dass die Polizei häufig vor dem Problem stehe, dass beim ersten Auftreten einer Person eine eindeutige Kategorisierung oder die Feststellung einer politischen Motivation „sehr schwierig ist“, dann deutet dies auf den Wunsch nach einer eher großzügigen Handhabung bzw. Speicherpraxis hin. Der Ausnahmecharakter einer Einspeicherung einer Person als „andere Person“ muss daher stärker betont werden; aufweichende Formulierungen sind insofern zu vermeiden. Wir haben dem LKA angekündigt, dass wir uns eine erneute Überprüfung der polizeilichen Speicherpraxis zu gegebener Zeit vorbehalten, wenn hinreichende Erfahrungen mit den Orientierungshilfen gewonnen worden sind.

Wir haben das LKA auch darauf hingewiesen, dass die gesetzlichen Anforderungen für jedes personenbezogene Datum, das gespeichert werden soll, gesondert zu prüfen sind. Wir halten daher die Speicherung zwar politisch motivierter, jedoch für sich betrachtet strafrechtlich nicht relevanter Handlungen für unzulässig, insbesondere soweit darin die zulässige Wahrnehmung von Grundrechten zum Ausdruck kommt, wie zum Beispiel die Teilnahme an nicht verbotenen (politischen) Versammlungen, die Verteilung von Flugblättern, das Betreiben von Informationsständen usw. Angaben hierüber dürfen in die AD PMK nicht aufgenommen werden, auch wenn die betreffende Person wegen anderer, politisch motivierter und strafrechtlich relevanter Vorkommnisse dort zulässigerweise gespeichert sein mag. Im Entwurf der Orientierungshilfen war zwar vorgesehen, dass im Fall der Wahrnehmung von Grundrechten (z. B. Antrag auf Einbürgerung, Religionsausübung, Teilnahme an politischen Veranstaltungen und Demonstrationen usw.) eine Speicherung personenbezogener Daten grundsätzlich nicht zulässig sein sollte, jedoch nur, sofern ansonsten keine weiteren Erkenntnisse vorliegen. Diese Formulierung ist zumindest missverständlich, lässt sie doch befürchten, dass bei einschlägig verdächtigen Personen unterschiedslos auch legale Verhaltensweisen erfasst und gespeichert werden.

## 5. Neues vom Lagebildinformationssystem der Polizei

Bereits im 24. Tätigkeitsbericht (LT-Drucksache 13/2650) hatten wir uns mit dem Lagebildinformationssystem der baden-württembergischen Polizei (LABIS) befasst, das seinerzeit als Prototyp im Bereich der damaligen Landespolizeidirektion Stuttgart I von der Polizeidirektion Böblingen erprobt wurde. LABIS soll die Erstellung aktueller Lagebilder erleichtern, aber auch die typische polizeiliche Aufgabenerfüllung, also z. B. die Verfolgung und vorbeugende Bekämpfung von Straftaten, unterstützen. Dazu verfügt das System über eine Lagebild- und eine Abfrage- bzw. Auswertekomponente. Die beiden Komponenten greifen auf eine Datenbank zurück, in der die täglichen Vorkommnisberichte der Polizeidienststellen gespeichert werden. Diese Vorkommnisberichte betrafen im Pilotprojekt ganz unterschiedliche Ereignisse; Straftaten waren dort ebenso verzeichnet wie Ordnungswidrigkeiten, Verkehrsunfälle, Beschwerden wegen Ruhestörungen, Ehestreitigkeiten oder Vermisstenanzeigen. Dementsprechend waren die in LABIS eingespeicherten Personen auch in ganz unterschiedlichen Zusammenhängen erfasst worden: Mutmaßliche Straftäter waren dort ebenso zu finden wie Geschädigte, Anzeigeerstatter, Zeugen, Unfallbeteiligte, Hinweisgeber oder Auskunftspersonen. Mit anderen Worten: Der flüchtige Ausbrecher konnte dort ebenso auftauchen wie der brave Bürger, der sich auf dem Revier über lärmende Nachbarn beschwerte.

Klar ist, dass ein so umfassendes Datenbanksystem wie LABIS erhebliche datenschutzrechtliche Risiken mit sich bringt; insbesondere die weitreichenden Recherchemöglichkeiten strapazieren das Zweckbindungsgebot und den Grundsatz der Erforderlichkeit nicht unerheblich. Wir hatten daher – wie im 24. Tätigkeitsbericht nachzulesen ist – eine Reihe von datenschutzrechtlichen Forderungen aufgestellt; sie betrafen die zeitlich begrenzte Speicherdauer der Vorkommnisberichte in der LABIS-Datenbank, die Vergabe von maßgeschneiderten Zugriffsberechtigungen für unterschiedliche Nutzergruppen, die sorgfältige Prüfung der Weitergabe der in LABIS gespeicherten Daten und die Protokollierung der Datenbankabfragen für Kontrollzwecke. Die Forderungen wurden damals aufgegriffen. LABIS wurde anschließend vom Innenministerium für den lokalen Einsatz bei den Polizeidirektionen freigegeben.

Flankierend hierzu wurden zur verbesserten Kriminalitätsbekämpfung auf Kreis-, Bezirks- und Landesebene, d. h. bei den Polizeidirektionen bzw. -präsidien, den Landespolizeidirektionen und beim Landeskriminalamt spezielle Stabsstellen (Zentrale Integrierte Auswertung – ZIA) – nachfolgend Stabsstelle genannt – eingerichtet, die die Aufgabe erhielten, mit Hilfe von LABIS und anderen Quellen ein tägliches aktuelles Lagebild zu erstellen; daneben sollten die Stabsstellen alle polizeilich relevanten Erkenntnisse zusammenführen und auswerten, um Tatserien und Tatzusammenhänge erkennen und Anregungen für Fahndungs- und Präventionsansätze geben zu können. Sie sollten im 4. Quartal 2005 den landesweiten Wirkbetrieb aufnehmen.

Mit der hierfür erforderlichen Vernetzung der Kreissysteme zu einem landesweiten Lagebildinformationssystem (LABIS-Land) und den zentralen Recherchemöglichkeiten kamen auf den Datenschutz qualitativ neue Herausforderungen zu. Dies hatte wohl auch das Landeskriminalamt erkannt, denn es legte uns Anfang Dezember 2005 ein „Datenschutz- und Sicherheitskonzept“ für LABIS-Land vor. Teilweise entsprachen die konzeptionellen Vorschläge bereits unseren früheren Anforderungen. Andererseits stellte sich in einer Besprechung im Dezember 2005, an der auch das Innenministerium teilnahm, heraus, dass die Landespolizeidirektionen inzwischen eigene Wege gegangen waren und die kreisübergreifende Nutzung des Lagebildinformationssystems durchaus unterschiedlich – und anders als im Datenschutz- und Sicherheitskonzept vorgesehen – ausgestaltet hatten. Besonders weit war dabei die Landespolizeidirektion Karlsruhe vorgeprescht. Das dortige Verfahren haben wir uns im Rahmen eines Kontrollbesuchs im Februar 2006 näher angeschaut.

### 5.1 Die Erstellung polizeilicher Lagebilder mit LABIS

Um Missverständnisse zu vermeiden: Grundsätzlich bestehen keine Bedenken, wenn sich die Polizei des Landes zur Bewältigung ihrer komplexen Aufgaben auf moderne Systeme der elektronischen Datenverarbeitung stützt, die in der Lage sind, aktuelle Lagebilder zu generieren, aus denen rasch Maßnahmen zur Gefahrenabwehr oder Strafverfolgung abgeleitet werden können. Soweit diese Systeme (aggregierte) Erkenntnisse ohne personenbezogene Daten wiedergeben (z. B. Schilderung wichtiger Ereignisse, Darstellung neuartiger Formen der Tatbegehung, statistische Entwicklung von Fallzahlen, auch im Vergleich verschiedener polizeilicher Dienststellen untereinander), sind sie datenschutzrechtlich unbedenklich. Personenbezogene Daten sollten in diese Lageberichte nur insoweit aufgenommen werden, wie es um Straftaten von erheblicher Bedeutung geht (so wie es etwa bei der Wiedergabe von Fahndungsmeldungen geschieht); diese Auffassung vertrat auch das Innenministerium. Da die personenbezogenen Daten aber ungeprüft in die Vorkommnisberichte einfließen und aus diesen in die Lageberichte gelangen können, empfahlen wir dem Innenministerium, bei der Aufnahme von personenbezogenen Daten in die Lageberichte auch in diesen Fällen besonderes Augenmerk auf die Wortwahl zu legen, insbesondere durch Zusätze wie „mutmaßlich“ o. Ä. deutlich zu machen, dass ein etwaiger Tatverdacht auf ungesicherten Erkenntnissen beruht.

Dementsprechend hatten wir auch der Freigabe des Moduls I von LABIS (Lagebildmodul) im Frühjahr 2003 zugestimmt. Denn dieses enthält – worauf auch das Datenschutz- und Sicherheitskonzept hinweist – ausschließlich fallbezogene Statistikdaten. Im Gegensatz dazu verfügt das Modul II über die jeweilige fallbezogene Sachverhaltsdarstellung sowie die personenbezogenen Daten der Betroffenen, wobei es sich – zumindest ausweislich des Datenschutz- und Sicherheitskonzepts – „nur“ um Beschuldigte im Rahmen eines strafrechtlichen Ermittlungsverfahrens oder aber um Polizeipflichtige im Rahmen der Gefahrenabwehr handeln sollte, also ein deutlich engerer Personenkreis als der, den wir noch im Pilotprojekt 2003 und – so viel sei verraten – auch bei unserem Kontrollbesuch bei der Landespolizeidirektion Karlsruhe zu sehen bekamen.

Bei unserem Besuch im Februar 2006 wurde uns zunächst der – datenschutzrechtlich relativ unkritische – Prozess der Erstellung des täg-

lichen landesweiten Lagebilds – Arbeitstitel „Tägliche Lage BW“ – auf der Ebene der Landespolizeidirektion erläutert. Die Stabsstelle der Landespolizeidirektion hatte dabei die Aufgabe, aus den bis 10 Uhr eingehenden Berichten der Kreisdienststellen einen Beitrag der Landespolizeidirektion für den ganzen Regierungsbezirk zusammenzustellen und diesen bis 12 Uhr an das Landeskriminalamt für das landesweite Lagebild weiterzuleiten. Das Lagebild wurde dann auch in das polizeiliche Intranet eingestellt. Bei der Erstellung des landesweiten Lagebilds stand erkennbar die allgemeine Kriminalität im Vordergrund, wobei das Hauptmeldeaufkommen über die Schutzpolizei kam. In diesem Zusammenhang wurde uns erläutert, dass es für den Staatsschutzbereich einen eigenen Meldeweg und eine eigene Datenbasis (AD PMK) gebe und dass sich die Stabsstelle auch nicht mit Falschgelddelikten befasse, weil hierfür ein eigener Meldedienst bestehe.

Die Berichte der Kreisdienststellen, die sich grundsätzlich auf Vorkommnisse mit überörtlicher Relevanz beschränken sollten, bildeten für die Stabsstelle der Landespolizeidirektion Karlsruhe jedoch nur einen Teil des verwendeten Materials; ebenso wurden z. B. Meldungen von Bundesdienststellen oder aus dem benachbarten Ausland verwendet. Einen erheblichen Anteil der Lageberichte machten daneben die Ergebnisse eigener Recherchen aus, die in den Vorkommnisberichten der nachgeordneten Dienststellen mit Hilfe der Abfragekomponente von LABIS durchgeführt wurden. Wenn man sich den Polizeialltag vor Augen hält, dann wird deutlich, welche gewaltige Menge an Informationen LABIS täglich bewältigen muss, aber auch, welche früher unvorstellbaren Recherchemöglichkeiten sich hierdurch eröffnen.

5.2 Die Auswertung der polizeilichen Vorkommnisberichte mit Hilfe von LABIS

Im Regierungsbezirk Karlsruhe konnte die Landespolizeidirektion – wie uns gezeigt wurde – mit Hilfe von LABIS bereits kreisübergreifend auf die Vorkommnisberichte der Kreisdienststellen zugreifen und durch Suchfunktionen (Volltextrecherche in allen Datenfeldern) personenbezogene Daten in ganz unterschiedlichen Zusammenhängen herausfiltern. Die uns am Bildschirm vorgeführten Recherchemöglichkeiten überschritten in mancherlei Hinsicht aber die Grenze des datenschutzrechtlich Zulässigen und bewegten sich auch außerhalb des im Datenschutz- und Sicherheitskonzept konzeptionell vorgedachten Rahmens: Im Unterschied zu den beiden Landespolizeidirektionen in Freiburg und Tübingen, die nach Aussagen des Innenministeriums bei ihren Analysen auf personenbezogene Auswertungen verzichteten, war die Landespolizeidirektion Karlsruhe in der Lage, eine retrograde Auswertung von personenbezogenen Daten bezirksweit bis auf die Ebene der von den örtlichen Polizeidienststellen im System „M-Text“ (künftig im System „ComVor“) angelegten Vorkommnisberichte vorzunehmen. Vereinfacht ausgedrückt, verfügte die Landespolizeidirektion Karlsruhe hier über eine regelrechte „Suchmaschine“, wie sie auch dem normalen Internetnutzer bekannt ist. So ließen wir von der Stabsstelle der Landespolizeidirektion in der Funktion „Einzelauswertung“ von LABIS einen willkürlich ausgewählten Namen („Müller“) unter einem bestimmten Datum („16.02.06“) eingeben; weitere Suchkriterien wären z. B. Ort, Ereignis, Straftatenschlüssel, modus operandi gewesen. Das System zeigte daraufhin in einer „Ergebnisliste“ alle „Treffer“, d. h. Hinweise auf Vorkommnisberichte an, in denen der Name „Müller“ unter dem vorgegebenen Datum auftauchte. Auf der Ebene der „Ergebnisliste“ war – soweit festgestellt – zwar noch kein Name zu lesen, allerdings hätte aus den dort teilweise wiedergegebenen vollständigen Anschriften unter Umständen ein Personenbezug abgeleitet werden können. Die unter den Suchbegriffen „Müller“ und „16.02.06“ aufgerufenen Vorkommnisse waren von ganz unterschiedlicher Art und Aussagekraft:

– So ging es in einem Vorkommnis auf der Ergebnisliste in Stichworten um einen nächtlichen Wildunfall auf der Gemarkung von Oberderdingen. Der Wechsel in die Detailsicht („Datensatzansicht“) machte dann deutlich, dass ein bestimmter Autofahrer (mit Angabe von Namen,

Anschrift und Geburtsdatum) mit einem Reh zusammengestoßen war, welcher Schaden an dem Fahrzeug (mit Angabe von Typ und Kennzeichen) entstanden war und was die Polizei nach dem Unfall unternommen hatte (Absicherung der Unfallstelle und Verständigung des namentlich aufgeführten Jagdpächters). Erst die Angaben zum Fahrzeug verrieten, warum das System einen Treffer vermeldet hatte: Das Fahrzeug war nämlich auf eine Firma aus dem Landkreis Karlsruhe zugelassen, in deren Namen das Wort „Müller“ vorkam.

– Das zweite Beispiel zeigte auf der Ergebnisliste – ohne personenbezogene Daten – nur das Stichwort „erkennungsdienstliche Behandlung“ um 21.15 Uhr. Wer vermutet hatte, die Detailsicht würde dieses Mal einen Tatverdächtigen namens Müller ausweisen, sah sich abermals getäuscht: Es handelte sich um einen (namentlich aufgeführten) türkischen Asylbewerber, der sich wegen eines mutmaßlichen Verstoßes gegen das Aufenthaltsgesetz einer erkennungsdienstlichen Behandlung unterziehen musste; jedoch hatte ein Polizeibeamter namens Müller dies angeordnet und war deshalb in dem Vorkommnisbericht namentlich und – wie die Stichprobe ergab – auch für übergeordnete Dienststellen recherchierbar in LABIS verewigt worden.

– Nach dem gleichen Muster wiesen auch die übrigen Treffer Personen namens „Müller“ unter dem Datum 16.02.06 aus, z. B. als Beteiligte mehrerer „VU“ (Verkehrsunfälle) unterschiedlichen Ausmaßes mit Personen- oder Sachschäden, wegen Fahrens unter Alkoholeinfluss oder wegen eines Ladendiebstahls. Dabei ging es nicht nur um Tatverdächtige, die diesen Namen trugen, sondern auch um Unfallgeschädigte, Kfz-Halter, Anzeigeerstatter oder Polizeibeamte. In einem Fall kam der Name „Müller“ sogar in einem Straßennamen vor. Straftaten wechselten sich ab mit anderen Vorkommnissen aus dem vielfältigen Arbeitsalltag der Polizei. So meldete eine namentlich erfasste Person offenbar wegen der Furcht vor der Vogelgrippe den Fund eines toten Eichelhähers, in einer anderen Meldung wurde über den Sturz eines älteren Mitbürgers auf der Straße berichtet, ein falscher Alarm wurde ebenso erfasst wie die Feststellung, dass bei einem kontrollierten Sattelzug die rückwärtige Beleuchtung defekt war. Stets enthielten die in LABIS gespiegelten Vorkommnisberichte an irgendeiner Stelle das gesuchte personenbezogene Datum.

Außerdem überprüften wir die Speicherdauer der personenbezogenen LABIS-Daten, die für die Mitarbeiter der Stabsstelle ein Jahr betragen soll. Zu diesem Zweck wurden alle Vorkommnisse vor dem 31. Dezember 2004 aufgerufen. Bei diesen hätte zum Zeitpunkt der Abfrage die Detailansicht ausgeblendet sein müssen. Dies war – soweit im Rahmen der Stichprobe feststellbar – auch der Fall. Fatal war nur, dass bereits auf der Ergebnisliste – also ohne Aufrufen der Detailansicht – in einem Fall als Vorkommnis unverblümt eine Verletzung der Unterhaltspflicht und eine bestimmte Adresse in Schwetzingen angegeben war. Es ist daher zu vermuten, dass auch in anderen Fällen detaillierte Adressenangaben in der Ergebnisliste eine Identifizierung der Betroffenen ermöglichen. Nun ist nicht abzustreiten, dass die Verletzung der Unterhaltspflicht ein strafrechtliches Vergehen nach § 170 des Strafgesetzbuchs ist und dass die Polizei eine entsprechende Strafanzeige eines/r Unterhaltsberechtigten in ihrem Vorgangsbearbeitungssystem aufnehmen darf. Für die Einspeicherung von Straftatverdächtigen (bei denen allerdings noch eine Wiederholungsgefahr bestehen muss), kann die Polizei jedoch personenbezogene Daten nach § 38 PolG in ihrem polizeilichen Auskunftssystem (POLAS BW) speichern, das extra für diesen Zweck geschaffen wurde. Das sollte für die polizeilichen Zwecke eigentlich ausreichen. Die zusätzliche Speicherung der Information in LABIS, dass eine bestimmte Person (bereits über die Adresse in der Ergebnisliste wäre ggf. der Täter zu ermitteln gewesen) eine Unterhaltspflichtverletzung begangen haben soll, ist – jedenfalls aus unserer Sicht – auf Ebene der Landespolizeidirektionen für Zwecke der Straftatenverfolgung oder der Gefahrenabwehr nicht erforderlich. Bei derartigen Delikten stellt sich anders als beispielsweise auf dem Feld der Organisierten

Kriminalität oder Rauschgiftkriminalität ohnehin die Frage, welche „Tatserien“ oder „Tatzusammenhänge“ durch zentrale Polizeidienststellen aufgehellt werden sollen. Die Recherchemöglichkeiten in LABIS sollten daher auf Straftaten von einigem Gewicht reduziert werden.

Als wir im Rahmen unseres Kontrollbesuchs nach dem Sinn der weitreichenden Recherchemöglichkeiten in LABIS fragten, wurden uns noch weitere Beispiele und Anwendungsfälle für Recherchen mit Hilfe von LABIS genannt:

– Tatzusammenhänge bzw. Tatserien könnten anhand der Beschreibung bestimmter, für sich betrachtet strafrechtlich nicht relevanter Vorkommnisse besser erkannt werden. Als Beispiel wurde die Meldung in einem Vorkommnisbericht genannt, dass bei einer Verkehrskontrolle im Kofferraum eines kontrollierten Fahrzeugs (dessen Fahrzeuginsassen und -Kennzeichen vermerkt werden) zahlreiche Außenspiegel bekannter Luxus-Autos gefunden wurden. Diese als „verdächtige Wahrnehmung“ gespeicherte Meldung könne zum Anlass genommen werden, eine Recherche in LABIS unter dem Stichwort „Außenspiegel“ zu starten, um Meldungen über ungeklärte Straftaten an Kraftfahrzeugen finden zu können. Auf diese Weise könne die Meldung über eine „verdächtige Wahrnehmung“ (Außenspiegel im Kofferraum) zu weiteren Ermittlungsansätzen führen.

– Ein Drogenkurier habe angegeben, sein Lieferant heiße mit Vornamen „Mehmet“ und fahre ein Fahrzeug mit schweizerischem Kennzeichen. Wenn bei einer Fahrzeugkontrolle eine verdächtige Wahrnehmung in einem Vorkommnisbericht registriert werde und dabei als Vorname des Fahrers ebenfalls „Mehmet“ und beim Fahrzeug ein schweizerisches Kennzeichen festgehalten würden, dann sei über LABIS-Land eine Verknüpfung dieser unterschiedlichen und allein nicht ausreichenden Ermittlungsansätze möglich.

– In Münster sei ein Mann kontrolliert worden, der Kinder auf einem Kinderspielplatz in auffälliger Weise beobachtet habe. Eine Straftat habe nicht vorgelegen und eine Recherche im bundesweiten polizeilichen Informationssystem (INPOL-Z) habe zu keinem Ergebnis geführt. Die weiteren Nachforschungen hätten aber ergeben, dass es sich um einen Arzt aus dem Regierungsbezirk Karlsruhe gehandelt habe, der gerade zu einem Ärztekongress in Münster weilte und über den Eintragungen wegen des Verdachts von Straftaten gegen die sexuelle Selbstbestimmung im polizeilichen Auskunftssystem des Landes (POLAS-BW) vorlagen. Außerdem habe der zuständigen Polizeidienststelle ein Antrag auf Löschung der Daten über eine frühere erkennungsdienstliche Behandlung vorgelegen, der dann aufgrund der neuen Meldung abgelehnt worden sei. Ohne die Vorkommnismeldung aus Münster wären die erkennungsdienstlichen Daten gelöscht worden. Der Bericht aus Münster sei zudem genutzt worden, um den Mann auf den Vorfall in Münster anzusprechen. Derartige Gefährderansprachen seien aufgrund der Vorkommnisberichte gezielter möglich. Warum der Mann nicht in INPOL-Z gespeichert war, vermochten die Gesprächspartner allerdings nicht zu erklären.

– Bei Verkehrsunfällen mit Sachschäden sei es sinnvoll, auch die Namen der Geschädigten im Vorkommnisbericht zu erfassen (und damit landesweit recherchierbar zu machen), um Tätern auf die Spur zu kommen, die Verkehrsunfälle zulasten der Versicherung vortäuschen bzw. manipulieren. Ergänzend hierzu ist anzumerken, dass – wie uns ein Polizeibeamter zutrug – die polizeilichen Sachbearbeiter selbst bei Kleinstunfällen ein spezielles Unfallaufnahmeblatt ausfüllen müssen, auf dem – ohne konkrete Verdachtsmomente – die Daten der Halter aller am Unfall beteiligten Fahrzeuge einzutragen sind. Wenn ein Haltername häufig auftauche, könne dies mit Hilfe von LABIS-Land festgestellt und zum Anlass für weitere Ermittlungen gemacht werden. Außerdem sollen die Polizeidienststellen aufgefordert worden sein, bei Fahrzeugkontrollen nicht nur die Daten von Fahrer und Fahrzeug, sondern auch die Personalien der Beifahrer in den Vorkommnisberichten festzuhalten.

5.3 Übers Ziel hinausgeschossen

Bei unserem Kontrollbesuch wurde rasch deutlich, dass das bei der Landespolizeidirektion Karlsruhe in Augenschein genommene System selbst dem Innenministerium und dem Landeskriminalamt zu weit ging. Denn bereits in dem zuvor vorgelegten Datenschutz- und Sicherheitskonzept vom Dezember 2005 waren wesentliche Einschränkungen vorgesehen. Das Innenministerium bestätigte uns denn auch im Oktober 2006, dass es unseren Anregungen in einigen Punkten – allerdings nicht in allen – Rechnung tragen wolle. Zugleich übersandte es uns das fortgeschriebene Datenschutz- und Sicherheitskonzept für LABIS (Version 3.0), an das sich jetzt alle betroffenen Polizeidienststellen halten sollen:

– Der Kreis der Betroffenen wird eingeschränkt. Die landesweit verwendete Version von LABIS soll künftig im Unterschied zu den lokalen LABIS-Anwendungen und auch zu dem bei der Landespolizeidirektion Karlsruhe konfigurierten LABIS-System auf Bezirksebene keine personenbezogenen Daten der Geschädigten, Zeugen, Hinweisgeber oder sonstigen Auskunftspersonen mehr enthalten. Derartige Daten sollen künftig auch nicht über Suchfunktionen und Volltextrecherche aus den Vorkommnisberichten (wo sie noch vorhanden sind) abrufbar sein. Diese Einschränkung ist grundsätzlich zu begrüßen, denn die bei unserem Kontrollbesuch namentlich aufgeführten Personen waren vielfach weder Straftatverdächtige noch Polizeipflichtige; für andere Zielgruppen erlaubt das Polizeigesetz nur in ganz begrenztem Umfang eine Datenspeicherung. Allerdings hält das Innenministerium den Zugriff z. B. auf die Daten von Unfallgeschädigten weiterhin grundsätzlich für erforderlich; derartige Daten müssten dann aber im Einzelfall „von Hand“ aus den Vorkommnisberichten ausgefiltert werden, was derzeit noch zu aufwendig sei. Deshalb habe man sich dazu entschlossen, die Personengruppe der Geschädigten, Zeugen, Hinweisgeber oder sonstigen Auskunftspersonen komplett auszuklammern. Die Polizeidienststellen sollen die Freitextfelder auch nicht mehr mit Angaben über diese Personengruppen versehen. Im Gegensatz dazu hatte die Stabsstelle der Landespolizeidirektion Karlsruhe eine große Menge an personenbezogenen Daten aus den lokalen Vorkommnisberichten zu Gesicht bekommen, die sie weder für die Erstellung von Lageberichten noch für eigene Recherchen benötigte. Das Innenministerium hat inzwischen dafür gesorgt, dass die bei der Landespolizeidirektion Karlsruhe praktizierten weitreichenden Recherchemöglichkeiten auf das landeseinheitliche Maß, wie es nach dem Datenschutz- und Sicherheitskonzept für LABIS-Land vorgesehen ist, zurückgeführt werden. Am Rande sei bemerkt, dass die Polizei den Betroffenen natürlich in der Regel Auskunft über ihre Speicherung in LABIS zu geben hat.

– Wie der zweite Trefferfall (s. o.) gezeigt hat, sind die am jeweiligen Vorgang beteiligten Polizeibeamten im Vorkommnisbericht namentlich genannt, wodurch sie in LABIS recherchierbar werden. Aus unserer Sicht war die Notwendigkeit hierfür nicht ohne weiteres erkennbar; die Telefonnummer der Dienststelle und die jeweilige Tagebuch-Nummer des Vorgangs dürften für etwaige Rückfragen ausreichen. Das Innenministerium war hierzu anderer Meinung; es hielt den datenschutzrechtlichen Eingriff für vertretbar, zumal auch in anderen polizeilichen Anwendungen der Sachbearbeiter namentlich aufgeführt sei. Wir meinen hierzu: Selbst wenn andere Verfahren das in gleicher Weise vorsehen, muss man diese wenig datenschutzfreundliche Praxis nicht unbedingt fortsetzen. In jedem Fall müssen die Voraussetzungen des § 36 LDSG vorliegen, wonach personenbezogene Daten von Beschäftigten nur unter bestimmten Voraussetzungen verarbeitet werden dürfen.

– Einen Dissens gibt es auch hinsichtlich der Abgrenzung der Zugriffsberechtigten bei der Polizei. Unstreitig ist, dass nur die Stabsstellen in LABIS recherchieren dürfen und nicht jeder Polizeibeamte in einer x-beliebigen Dienststelle. Wir hatten außerdem angeregt, die Recherchemöglichkeiten vom Inhalt und von den Berechtigten her

ebenenspezifisch abzuschichten und beispielsweise den Kreis- und Bezirksdienststellen Recherchen nur für ihren jeweiligen Zuständigkeitsbereich zu erlauben. Das Innenministerium und das Landeskriminalamt hielten aus kriminologischen Gründen (u. a. wegen der Mobilität der Täter) eine landesweite Recherchemöglichkeit durch alle Mitarbeiter in den Stabsstellen (aller Dienststellen) für erforderlich. Demgegenüber hatte noch die Landespolizeidirektion Karlsruhe bei unserem Kontrollbesuch im Februar 2006 Wert darauf gelegt, dass nur die Stabsstelle der Landespolizeidirektion in den Vorkommnisberichten der nachgeordneten Dienststellen recherchieren kann, um den Überblick zu behalten. Das Landeskriminalamt meinte bereits damals, dies könne zu einer Überlastung der Stabsstelle der Landespolizeidirektion führen; Recherchen sollten deshalb durch jede Stabsstelle einer Polizeidirektion auch in den Vorkommnisberichten der anderen Polizeidienststellen möglich sein („Recherche durch alle bei allen“). Inzwischen hat sich offenbar das Landeskriminalamt mit seiner Auffassung durchgesetzt. Wir halten dies nicht für zwingend: Die Polizeiorganisation des Landes ist nicht ohne Grund hierarchisch aufgebaut und sieht funktional und örtlich zwischen den Polizeidienststellen getrennte Zuständigkeiten vor. Dementsprechend sollten auch die Recherchemöglichkeiten räumlich auf den jeweiligen Zuständigkeitsbereich beschränkt sein. Dies trägt zur sparsamen Verwendung von Daten bei und kann einen Datenmissbrauch verhindern helfen. Letztlich spiegelt ein Vorkommnisbericht die Vorgangsbearbeitung wieder. Inwieweit die Recherche durch eine Polizeidirektion in den Vorkommnisberichten einer hierarchisch auf gleicher Ebene stehenden anderen Polizeidirektion mit dem Zuständigkeitsbegriff des Polizeigesetzes noch zu vereinbaren ist, ist aus unserer Sicht fraglich. Die Möglichkeit einer Auswertung durch eine Polizeidirektion bei allen anderen Polizeidirektionen würde zudem die Zentralstellenfunktion des Landeskriminalamts (vgl. §§ 10, 11 DVO PolG) konterkarieren. Letztlich ist die Erforderlichkeit der landesweiten Recherche aber fachlich und organisatorisch vom Innenministerium zu beurteilen. Sofern allen Stabsstellen der Kreisdienststellen Recherchemöglichkeiten in den Vorkommnisberichten aller anderen Kreisdienststellen eingeräumt werden sollen, sollten entsprechende Recherchen protokolliert werden; außerdem sollte nach angemessener Zeit eine Evaluation erfolgen, in welchen Fällen tatsächlich kreisübergreifende Recherchen mit welchem Ergebnis angestellt wurden. Gegebenenfalls sind dann die Recherchemöglichkeiten wieder einzuschränken. Das Innenministerium will diese Anregung aufgreifen; Maßstab der Bewertung soll dann sein, inwieweit die Stabsstellen auf Polizeidirektions-Ebene tatsächlich mit Hilfe von LABIS kreisübergreifende Recherchen zur Aufdeckung von Tatserien und Tatzusammenhängen erfolgreich durchführen können.

– Die landesweite Recherchemöglichkeit der Mitarbeiter der Stabsstellen bleibt auf einen Zeitraum von zwölf Monaten beschränkt; die Recherche in der lokalen LABIS-Anwendung soll – wie bisher – (nur) den Polizeibeamten der betreffenden Polizeidirektion für einen Zeitraum von drei Monaten eingeräumt werden. Das von uns angesprochene Problem der Datenlöschung, sobald die Datenspeicherung nicht mehr erforderlich ist (z. B. weil ein Straftatverdacht sich als unbegründet erweist), wird aufgegriffen; in LABIS soll eine Einzelfall-Löschung ermöglicht werden.

– Der gewichtigste Dissenspunkt zwischen dem Innenministerium und uns war die Frage, welche der in den örtlichen Vorkommnisberichten erfassten Vorfälle überhaupt in LABIS-Land recherchierbar sein sollen. Das Innenministerium will nun erfreulicherweise auf die Einbeziehung personenbezogener Daten verzichten, die zum Zweck der Verfolgung von Ordnungswidrigkeiten oder zur Gefahrenabwehr erhoben wurden. Damit würden etliche der bei unserem Kontrollbesuch noch festgestellten „Treffer“ herausfallen. In einem anderen Punkt hat sich das Innenministerium leider nicht so entgegenkommend gezeigt: Es besteht weiterhin auf der Einbeziehung von per-

sonenbezogenen Daten im Zusammenhang mit sog. „verdächtigen Wahrnehmungen“. Wir sehen hier ein nur schwer zu beherrschendes Einfallstor für den Ausbau von LABIS zu einer polizeilichen Superdatenbank, in der alle aus Sicht der Polizei „auffälligen“ Verhaltensweisen eingespeichert und landesweit recherchierbar vorgehalten werden können. Die Abgrenzung ist auch nicht ganz stimmig, wenn auf der anderen Seite keine personenbezogenen Daten im Zusammenhang mit der Gefahrenabwehr und mit der Verfolgung von Ordnungswidrigkeiten eingespeichert werden sollen und mit POLAS-BW eine umfassende Datenbank über Straftatverdächtige zur Verfügung steht. Bei unseren Gesprächen in Karlsruhe wurde jedenfalls eingeräumt, dass der Begriff der „verdächtigen Wahrnehmung“ nur schwer einzugrenzen sei und in erster Linie Sachverhalte betreffe, bei denen aufgrund polizeilichen Erfahrungswissens der Verdacht in Richtung einer begangenen oder bevorstehenden Straftat gelenkt wird (Beispiel: Polizei findet bei einer Fahrzeugkontrolle typisches Diebesgut oder Einbruchswerkzeug). Soweit die „verdächtige Wahrnehmung“ dabei die Schwelle einer konkreten Gefahr oder eines Straftatverdachts nach §§ 37, 20 Abs. 2 bis 5 und § 38 PolG überschreitet, bestehen gegen eine entsprechende Datenspeicherung keine durchgreifenden datenschutzrechtlichen Bedenken. Eine Speicherung von personenbezogenen Daten in Dateien wie LABIS-Land außerhalb dieses Anwendungsbereichs ist aus unserer Sicht jedoch nicht zulässig. Die Datenspeicherung muss stets für die Abwehr einer konkreten Gefahr bzw. aufgrund eines bestehenden Straftatverdachts erforderlich sein. Eine Datenspeicherung nur aufgrund eines „unguten Gefühls“ bei den ermittelnden Polizeibeamten wäre zu unbestimmt und damit unzulässig. Sofern die personenbezogenen Daten lediglich im Rahmen der Vorgangsbearbeitung gespeichert werden, dürfen sie auch nicht für die „Hauptzwecke“ der polizeilichen Arbeit, die Gefahrenabwehr oder die vorbeugende Bekämpfung von Straftaten, verwendet werden. Vielmehr würde sich das Erheben und Speichern von Daten – wenn keine konkrete Gefahr oder kein konkreter Straftatverdacht vorliegen – als anlassloses Sammeln von Daten auf Vorrat darstellen, für das es einer speziellen Rechtsgrundlage bedarf. Eine Zustimmung zu dieser Vorgehensweise konnte unsererseits daher nicht erteilt werden. Das Innenministerium will die Schwelle hingegen nicht zu niedrig ansetzen und die „verdächtigen Wahrnehmungen“ der Polizei recherchierbar machen. Es bleibt nun abzuwarten, wie das Konzept in der Praxis umgesetzt wird. Wir wagen die Prognose: Die Polizeidatenbank LABIS wird uns weiter beschäftigen und auch in den kommenden Jahren in unserer Berichterstattung nicht unerwähnt bleiben.

### 6. Speicherung personenbezogener Daten durch die Polizei im Zusammenhang mit strafrechtlichen Ermittlungsverfahren

Die meisten Bürger, die unsere Dienststelle im Zusammenhang mit der Polizei anschreiben, wollen wissen, aus welchem Grund und für wie lange die Polizei ihre Daten aus zurückliegenden strafrechtlichen Ermittlungsverfahren speichern darf. Auslöser für diese Anfragen ist häufig, dass die Betroffenen bei irgendwelchen Polizeikontrollen von den Polizeibeamten mehr oder weniger diskret, manchmal leider auch in Gegenwart nichts ahnender Dritter, damit konfrontiert werden, dass sie der Polizei bereits bekannt und deswegen im Polizeicomputer erfasst seien. Wenn es sich dann noch um ein Verfahren wegen eines Betäubungsmitteldelikts gehandelt hatte und der betroffene Bürger mit einem Fahrzeug unterwegs ist, kann er mit einiger Sicherheit damit rechnen, dass dem Hinweis auf die vermeintlich dunkle Vergangenheit eine gründliche und zeitraubende Durchsuchung des Fahrzeugs folgen wird. Viele Bürger sind in solchen Situationen nicht nur wegen der überraschten Beifahrer(-in), sondern vor allem deswegen aufgebracht, weil sie nie rechtskräftig verurteilt worden sind und aufgrund fehlender Eintragungen im Bundeszentralregister angenommen hatten, gegenüber dem Staat eine „weiße Weste“ zu haben. Wir müssen diese Bürger dann regelmäßig darüber aufklären, dass ein makelloses Führungszeugnis noch lange nicht bedeutet, in den Informationssammlungen der Polizei nicht

mit dem „Grauschleier“ eines Straftatverdachts behaftet zu sein. Der Polizeivollzugsdienst kann nämlich auf der Grundlage von § 38 des Polizeigesetzes (PolG) Daten, die ihm im Rahmen von Ermittlungsverfahren bekannt geworden sind, speichern und nutzen, soweit und solange dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Dies ist der Fall, wenn die betroffene Person verdächtig ist, eine Straftat begangen zu haben, und tatsächliche Anhaltspunkte dafür vorliegen, dass sie zukünftig eine Straftat begehen wird. Auf Landesebene werden die erhobenen Daten in der Regel im Polizeilichen Auskunftssystem (POLAS-BW) gespeichert. Ein Straftatverdacht kann nach der ständigen Rechtsprechung der Verwaltungsgerichte sogar dann bejaht werden, wenn das Ermittlungsverfahren von der Staatsanwaltschaft oder vom Gericht eingestellt, der Straftatverdacht dabei aber nicht gänzlich ausgeräumt worden ist. Darin liegt auch der wesentliche Unterschied zur Speicherung von rechtskräftigen Verurteilungen im Bundeszentralregister, das bei Führungszeugnissen abgefragt wird. Selbst durch einen Freispruch aus Mangel an Beweisen wird – wie das Bundesverfassungsgericht einmal festgestellt hat – ein Tatverdacht nicht generell ausgeschlossen; allerdings bedürfe es hier einer besonders gründlichen Prüfung des Einzelfalls unter Berücksichtigung der Gründe der Entscheidung. Die Unschuldsvermutung im Strafprozess stehe dem übrigens nicht entgegen, da die Feststellung eines Tatverdachts etwas substantiell anderes sei als eine Schuldfeststellung (vgl. Bundesverfassungsgericht, Beschluss vom 16. Mai 2002, 1 BvR 2257/01, RDV 2003, S. 80).

Diese Rechtslage kann im Extremfall dazu führen, dass etwa in einem Nachbarstreit mit wechselseitigen Strafanzeigen (zum Beispiel wegen Beleidigung) beide Kontrahenten im Polizeicomputer gespeichert werden, obwohl der genaue Geschehensablauf unklar ist und im Strafverfahren auch nicht aufgeklärt wird, weil die Staatsanwaltschaft derartige Strafverfahren regelmäßig einstellt und die Streithähne auf den Privatklageweg verweist. Aus Sicht der Polizei bleibt in diesen Fällen der Makel des Straftatverdachts an beiden Beteiligten haften. Ob die massenhafte Einspeicherung derartiger Bagatelldelikte tatsächlich zur vorbeugenden Bekämpfung von Straftaten geeignet ist, muss ernsthaft bezweifelt werden. Da auch die Hürden für die Annahme einer Wiederholungsgefahr relativ niedrig sind, tummeln sich auf diese Weise zahlreiche Bürger – vermutlich ohne es zu wissen – in den polizeilichen Datenbanken. Aus unserer Sicht ist dies ein bedenklicher Zustand und wir können daher denjenigen, die mal in ein Ermittlungsverfahren verwickelt waren und sich nicht sicher sind, inwieweit sie in polizeilichen Dateien erfasst sind, nur empfehlen, bei der Polizei eine Auskunft über ihre Daten zu beantragen: diese muss die Polizei übrigens kostenlos erteilen.

Bei unseren Recherchen stoßen wir in diesem Zusammenhang immer wieder auf das Problem, dass die polizeilichen Informationssysteme – in Baden-Württemberg also POLAS-BW – die Vorgeschichte leider nur knapp widerspiegeln und die um Stellungnahme gebetene Polizeidienststelle das Ergebnis eines strafrechtlichen Ermittlungsverfahrens nicht mehr feststellen kann. Vielfach handelt es sich dabei um lange zurückliegende Datenspeicherungen aus den 80er- oder frühen 90er-Jahren, als die Übermittlung der staatsanwaltschaftlichen oder gerichtlichen Entscheidungen an die Polizei vermutlich lückenhafter als heute war. Die Daten sind nur deswegen noch gespeichert, weil vor Ablauf der Überprüfungsfrist neue Ermittlungsverfahren eingespeichert wurden. Auch im Hinblick auf den inzwischen verstrichenen Zeitraum wäre unseres Erachtens in diesen Fällen eine Löschung der nicht vollständig dokumentierten Vorgänge angebracht. Der Informationsverlust für die Polizei dürfte nur gering sein; demgegenüber wäre der Aufwand für die Vervollständigung der lückenhaften Unterlagen erheblich. In der Praxis wurden wir mit unterschiedlichen Fallkonstellationen konfrontiert:

– In einigen Fällen waren überhaupt keine Akten mehr vorhanden. Wir haben daraufhin unter Berufung auf die datenschutzrechtliche Grundregel einer hinreichenden Dokumentation der Gründe für die Datenspeicherung eine Löschung der entsprechenden Daten gefordert (vgl. zum Beispiel die entsprechenden Hinweise zur Arbeitsdatei „Politisch motivierte Kriminalität“ im 26. Tätigkeitsbericht, LT-Drucksache 13/4910).

– In einigen anderen Fällen hat die betroffene Polizeidienststelle erklärt, dass der Verfahrensausgang zwar nicht mehr feststellbar sei, weil die (abschließenden) staatsanwaltschaftlichen oder gerichtlichen Entscheidungen in den Akten fehlen würden, dass aus den Ermittlungsakten aber der Tatverdacht gegen den Betroffenen in Form von Geständnissen, Zeugenaussagen, Berichten des damaligen Sachbearbeiters usw. hervorgehe.

– In weiteren Fällen wurden mangels schriftlicher Belege Gespräche mit dem damaligen Sachbearbeiter geführt, der dann aus der Erinnerung heraus den Tatverdacht bzw. eine Wiederholungsgefahr bestätigen sollte.

Die geschilderte Polizeipraxis verstieß unseres Erachtens in allen drei Fallkonstellationen gegen die datenschutzrechtliche Grundregel, wonach die Erforderlichkeit einer Speicherung personenbezogener Daten in einer automatisierten Datei in den zugrunde liegenden Akten vollständig dokumentiert sein muss. Nach Nr. 4 VwV PolG zu § 38 ist nämlich die Frage, ob nach dem Abschluss des Ermittlungsverfahrens noch ein begründeter Tatverdacht besteht, „unter Berücksichtigung der Entscheidung der Staatsanwaltschaft oder des Gerichts anhand aller Umstände des Einzelfalls“ zu beantworten. Fehlt die (abschließende) staatsanwaltschaftliche oder gerichtliche Entscheidung in den polizeilichen Unterlagen, so kann die Entscheidung über die Erforderlichkeit der (weiteren) Datenspeicherung nicht hinreichend begründet bzw. durch Dokumente belegt werden. Falls es nicht gelingt, die Dokumentation durch die Beschaffung der fehlenden staatsanwaltschaftlichen oder gerichtlichen Entscheidungen wieder zu vervollständigen, sind die Datenspeicherungen in diesen Fällen zu löschen. Die Befragung ehemaliger Sachbearbeiter zur Rekonstruktion früherer Ermittlungsergebnisse stellt dabei keine zulässige Form der Vervollständigung einer lückenhaften Dokumentation dar. Eine Löschung der gespeicherten Daten ist unabhängig davon in allen Fällen zwingend vorzunehmen, in denen überhaupt keine Akten mehr vorhanden sind, die die Erforderlichkeit der Datenspeicherung belegen. Damit wir uns nicht in jedem Einzelfall stets von neuem mit den Polizeidienststellen herumstreiten müssen, haben wir das Innenministerium um eine generelle Klärung und entsprechende Weisung an die nachgeordneten Dienststellen gebeten.

Das Innenministerium hat daraufhin in einem Erlass vom Mai 2006 einigen unserer Bedenken Rechnung getragen:

– Das Innenministerium hat die nachgeordneten Polizeidienststellen darauf hingewiesen, dass in denjenigen Fällen, in denen keine Akten mehr vorhanden sind, die entsprechenden Datensätze zu löschen sind. Die fehlende Dokumentation könne auch nicht durch eine Befragung und einen hierüber angefertigten Vermerk des damaligen Sachbearbeiters, der dann aus der Erinnerung heraus den Tatverdacht bzw. die Wiederholungsgefahr bestätigen soll, ersetzt werden.

– In den Fällen, in denen die Akten zwar noch vorliegen, aber der Ausgang des Verfahrens nicht mehr feststellbar ist, weil die abschließenden staatsanwaltlichen oder gerichtlichen Entscheidungen in den Akten fehlen, solle differenziert verfahren werden: Zunächst sei zu prüfen, ob auf die weitere Speicherung, insbesondere im Hinblick auf den verstrichenen Zeitraum, verzichtet werden kann. Wenn nach dieser Prüfung keine Löschung erfolgen soll, solle sich die Dienststelle zunächst um eine Vervollständigung der Akten bemühen und die abschließende staatsanwaltschaftliche oder gerichtliche Entscheidung beschaffen. Wenn auch dieses nicht gelingt, solle geprüft werden, ob sich aus der polizeilichen Aktenlage ein fortbestehender Tatverdacht ergibt. Im Zweifel solle der Löschung der Daten der Vorzug gegeben werden.

– In Fällen von geringer Bedeutung, insbesondere wenn es sich um die erste und einzige Speicherung handelt, habe – auch bei fortbestehendem Tatverdacht – in der Regel eine Löschung zu erfolgen.

Das Innenministerium hat außerdem seine Polizeidienststellen daran erinnert, dass nicht nur beim Ablauf der Aussonderungsprüffristen, sondern auch im Rahmen der laufenden Sachbearbeitung stets zu prüfen sei, ob die der Speicherung zugrunde liegenden Akten, insbesondere über den Ausgang des Verfahrens, vorliegen.

Wir hoffen, dass diese Direktive nach und nach zu einer Entschlackung der polizeilichen Datensammlungen beitragen wird. Leider ist das Innenministerium bei seinem Standpunkt geblieben, dass der Straftatverdacht aus den Polizeiakten auch dann abgeleitet werden darf, wenn eine abschließende staatsanwaltschaftliche oder gerichtliche Entscheidung über den Verfahrensausgang weder vorliegt noch nachträglich beschafft werden kann. Es stützt sich dabei auf eine Entscheidung des Verwaltungsgerichts Sigmaringen, das diese Frage in einer Entscheidung aus dem Jahr 1994 – leider ohne weitere Begründung – bejaht hatte (Urteil vom 17. Januar 1994, 1 K 901/92). Wir halten die Argumentation für nicht überzeugend; sie entspricht auch nicht dem klaren Wortlaut der Verwaltungsvorschrift Nr. 4 zu § 38 PolG. Welche künftigen Straftaten die Polizei mit Hilfe solcher lückenhaften Uraltdaten verhindern will, bleibt ohnehin ihr Geheimnis.

**7. Datenbestand der DNA-Analyse-Datei beim Bundeskriminalamt fehlerhaft?**

In der DNA-Analyse-Datei beim Bundeskriminalamt (BKA) sind vor allem die Identifizierungsmuster aus molekulargenetischen Untersuchungen von Personen gespeichert, die einer Straftat von erheblicher Bedeutung oder einer Straftat gegen die sexuelle Selbstbestimmung verdächtig sind und bei denen angenommen wird, dass sie weitere bedeutsame Straftaten begehen könnten (vgl. § 81 g der Strafprozessordnung – StPO). Die Datei soll dadurch künftige Straftaten leichter aufklären helfen. Man sollte meinen, dass es ohne weiteres möglich ist, durch eine einfache Datenbankrecherche herauszufinden, wie sich die Datensätze auf bestimmte Anlassstraftaten verteilen. Weit gefehlt. Bereits im Jahr 2004 hatte das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein erfahren, dass eine Aufschlüsselung der Datei nach Straftaten nur auf Umwegen möglich ist; das dortige Landeskriminalamt hatte ihm nämlich mitgeteilt, dass rund 300 Systemabfragen über entsprechende Katalogwerte erforderlich seien. Abgesehen davon, dass jedes Delikt einzeln abgefragt werden müsse und die Recherche viele Stunden dauern werde, könne die Recherche nur bei ruhendem Normalbetrieb erfolgen. Es wurde daher angeregt zu prüfen, ob sich im Zuge der im Bundeskriminalamt anstehenden Migration zu INPOL-neu eine bessere Auswertbarkeit der DNA-Analyse-Datei erreichen lasse. Das BKA teilte daraufhin jedoch mit, auch nach der Migration der Datei in INPOL-neu seien Recherchen nur anhand der Oberbegriffe der einzelnen Abschnitte des Strafgesetzbuchs und der Bezeichnungen der Nebengesetze möglich.

Auf Wunsch der Datenschutzbeauftragten des Bundes und der Länder nahm schließlich das Bundeskriminalamt eine Auswertung der DNA-Analyse-Daten über den Gesamtbestand und die Zahlen für die einzelnen Bundesländer vor (Stand: Oktober 2004). Für Baden-Württemberg waren zum damaligen Zeitpunkt in der DNA-Analyse-Datei insgesamt 65 641 Datensätze (mit belegtem Deliktsdatenfeld) erfasst. Auffallend war, dass eine ganze Reihe der Datenspeicherungen auf den ersten Blick nicht den Voraussetzungen des § 81 g StPO entsprach, da das jeweilige Deliktsdatenfeld weder eine Straftat von erheblicher Bedeutung noch eine Straftat gegen die sexuelle Selbstbestimmung enthielt. So waren dort u. a. 226 Datenspeicherungen unter dem Oberbegriff „Sachbeschädigung“, 14 Fälle unter dem Oberbegriff „Strafbarer Eigennutz“, acht Fälle wegen „Falscher Verdächtigung“ und 174 Fälle wegen „Widerstands gegen die Staatsgewalt“ verzeichnet. Die Auswertung bezog sich auf die Rechtslage, wie sie bis zum 1. November 2005 gegolten hatte; die Auflistung von Delikten mit geringerem Unrechtsgehalt konnte daher nicht auf die nunmehr nach der Strafprozessordnung erleichterten Voraussetzungen für die Erhebung und Speicherung von DNA-Daten zurückzuführen sein. Aus unserer Sicht mussten daher bei der Einspeicherung systembedingte oder individuelle Fehler passiert sein. Denn auch wenn der Gesetzgeber keinen abschließenden Katalog an Straftaten als Voraussetzung für die Datenspeicherung vorgegeben hat, so müssen als Voraussetzung für eine Einspeicherung in der DNA-Analyse-Datei doch Straftaten vorliegen, die von ihrem Unrechtsgehalt her und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit Straftaten von erheblicher Bedeutung gleichzusetzen sind (vgl. § 81 g Abs. 1 Satz 2 StPO).

Eine mögliche Ursache für die Speicherung geringfügiger Anlassstraftaten erfuhren wir aus einem anderen Bundesland: Danach schien es so zu sein, dass in der DNA-Analyse-Datei aus – wie es etwas verklausuliert hieß – „ermittlungs- und verfahrenstechnischen Gründen“ als Erfassungsgrund auch Straftaten ohne erhebliche Bedeutung gespeichert worden waren. So komme es beispielsweise bereits bei der Speicherung von Spuren am Tatort zur Festlegung einer Spurennummer. Wenn die anlässlich einer minderschweren Straftat gesicherte DNA-Spur mit einer erheblichen Straftat, zu der keine DNA-Spur vorliegt, zu einem Sammelvorgang verbunden wird, so werde die Spur in der DNA-Analyse-Datei weiterhin unter dem Ursprungsdelikt erfasst, um die Spurenzuordnung nicht zu gefährden. Zudem sei die Eingabe mehrerer Erfassungsgründe in der DNA-Analyse-Datei nicht möglich. Wenn diese Erklärung tatsächlich zutreffen sollte, dann wäre eine rasche Abhilfe geboten. Unseres Erachtens darf schon nach der Errichtungsanordnung zur DNA-Analyse-Datei in der Datei nur der der Einspeicherung zugrunde liegende Tatvorwurf gespeichert werden, der seinerseits den materiell-rechtlichen Voraussetzungen entsprechen muss. Die genannten Datenspeicherungen sind deswegen entweder zu korrigieren oder zu löschen. Die geschilderten „ermittlungs- und verfahrenstechnischen“ Probleme sind jedenfalls nicht durch die Speicherung unrichtiger Daten zu lösen.

Das von uns um Stellungnahme gebetene Innenministerium veranlasste daraufhin eine stichprobenweise Erhebung und Auswertung der Datensätze zu den oben genannten Deliktsgruppen durch das Landeskriminalamt. Dabei stellte sich heraus, dass die Datenspeicherungen zu „unpassenden“ Anlassstraftaten in der DNA-Analyse-Datei inzwischen weiter zugenommen hatten: Mittlerweile waren schon 323 Sachbeschädigungen, 17 Fälle von „strafbarem Eigennutz“, 14 Fälle wegen „falscher Verdächtigung“ und 261 Datensätze wegen Widerstands gegen die Staatsgewalt gespeichert (Stand: 15. März 2006). Bei den Sachbeschädigungen bezogen sich 123 Datenspeicherungen auf Spurendatensätze, bei der Deliktsgruppe „Falsche Verdächtigung“ war dies einmal der Fall, bei den beiden weiteren Deliktsgruppen ließ sich das Ergebnis jedenfalls nicht durch Spurendatensätze erklären, denn es waren hierzu keine gespeichert. Das Landeskriminalamt zog im Rahmen der Auswertung insgesamt 76 Stichproben und schaute sich die Fälle genauer an. Nur bei einer der Personen war die Datenerfassung nach dem 1. November 2005 erfolgt. Das Innenministerium und das Landeskriminalamt konnten die offensichtlich falsche Zuordnung der Anlassstraftaten auch nicht schlüssig erklären und hielten mehrere Ursachen für möglich. Uns wurde mitgeteilt, dass sich erst durch eine aufwendige Einzelfallprüfung unter Einbeziehung der Ermittlungsdienststellen feststellen lasse, inwieweit die materiell-rechtlichen Voraussetzungen für eine Erhebung und Speicherung der DNA-Daten vorlagen oder nicht. Immerhin kündigte das Innenministerium eine umfassende Überprüfung der DNA-Datensätze zu einigen einschlägigen Deliktsgruppen durch das Landeskriminalamt an, die allerdings bis zum Jahresende 2006 dauern werde. Unsere Bitte, die Einzelfallprüfung wenigstens hinsichtlich der vom LKA gezogenen Stichprobe vorzuziehen, blieb bis heute leider unbeantwortet.

## 8. Einzelfälle

### 8.1 Baskenterror im Nordschwarzwald? Die Überprüfung von Vereinen durch die Polizei

Im Januar 2006 erkundigte sich der Vorsitzende einer „Badisch-Baskischen Gesellschaft“ in einer nordbadischen Stadt bei uns, ob und warum die Polizei seinen Verein, der zur Unterstützung einer Städtepartnerschaft mit einer baskischen Stadt gegründet worden war, überprüfen darf. Bei dem Vereinsvorsitzenden hatte sich nämlich telefonisch eine Mitarbeiterin der örtlichen Kriminalpolizei gemeldet und mitgeteilt, dass sie aufgrund eines Erlasses des Innenministeriums routinemäßig Vereine überprüfe und ihm deshalb ein paar Fragen stellen wolle. Sie wollte von ihm einige Strukturdaten des Vereins wissen. Im Verlauf des Telefongesprächs stellte sich dann heraus, dass es darum ging, einen Fragebogen auszufüllen. Die Bitte, den Fragebogen und den

erwähnten Erlass zugesandt zu erhalten, wurde jedoch nicht erfüllt, weil die Kripobeamtin bei einem Rückruf erklärte, der Erlass sei intern und der Fragebogen nur per Telefon oder persönlich in der Dienststelle auszufüllen. Der Bürger, der die Beamtin darauf hinwies, dass die Aktivitäten des Vereins bei der Stadt bestens bekannt seien, und ihr außerdem den nicht ganz ernst gemeinten Vorschlag unterbreitete, sie möge auch den örtlichen Schachclub überprüfen, dessen Vorsitzender er ebenfalls sei, war nun nicht mehr zu einer Auskunft bereit und schaltete unsere Dienststelle ein. Dabei ließ er uns wissen, dass bei einem anderen Vereinsmitglied angeblich der Verfassungsschutz wegen Auskünften über den Verein vorgesprochen habe.

Auf Nachfrage gab uns das Innenministerium folgende Auskunft:

Die Anfrage beim Vereinsvorsitzenden sei nicht Teil einer größeren Aktion zur Abklärung ausländischer Vereine gewesen. Auslöser für die Aktion sei vielmehr eine Anfrage des Amts für öffentliche Ordnung der Stadt bei der zuständigen Polizeidirektion gewesen, ob dort Erkenntnisse über den Verein vorlägen. Beim dortigen Staatsschutz lag zwar nichts vor. Dennoch befragte eine Kriminalbeamtin, die nicht im Bereich Staatsschutz tätig war, telefonisch den Vereinsvorsitzenden. Sie habe sich dabei – offenbar in Ermangelung anderer Unterlagen – an einer „Führungs- und Einsatzanordnung zur intensivierten Bekämpfung krimineller Islamisten“ des Innenministeriums aus dem Jahr 2002 sowie an einer Checkliste, die zur Abklärung von Vereinen mit islamistischem Hintergrund verwendet wird, orientiert. Die Rechtsgrundlage hierfür sei § 20 Abs. 1 des Polizeigesetzes (PolG) gewesen. Eine Anfrage durch den Verfassungsschutz habe daneben nicht festgestellt werden können. Dem Amt für öffentliche Ordnung der Stadt sei inzwischen mitgeteilt worden, dass über den Verein keine Erkenntnisse in staatsschutzmäßiger Hinsicht vorliegen. Personenbezogene Daten seien in dieser Angelegenheit nicht gespeichert worden. Der Antwort des Innenministeriums war übrigens der besagte Erlass und der bei der telefonischen Anfrage offenbar verwendete „Vereinserhebungsbogen“ der Polizeidirektion (Kriminalpolizei, Staatsschutz) beigefügt worden.

So beruhigend die Auskunft des Innenministeriums einerseits war, so merkwürdig kam uns doch die scheinbar routinemäßige Recherche der Polizei bei einem Verein vor, der beim besten Willen nicht mit kriminellen Islamisten in Verbindung zu bringen war. Deshalb baten wir das Innenministerium um eine ergänzende Begründung, auf welcher Rechtsgrundlage der Polizeivollzugsdienst – unabhängig von einem vereinsrechtlichen Verbotsverfahren, für das die örtliche Ordnungsbehörde gar nicht zuständig wäre, und offenbar unabhängig vom Vorliegen von Anhaltspunkten für Aktivitäten krimineller Islamisten, auf die sich der o. g. Erlass des Innenministeriums bezog – Nachforschungen über eingetragene Vereine, die Zusammensetzung des Vereinsvorstands, die Vereinsmitglieder und die Aktivitäten des Vereins anstellt. Wir wollten außerdem wissen, wie und bei wie vielen Vereinen im Lande Überprüfungen aufgrund des Erlasses stattgefunden haben. Einige Zeit später ließ uns der Vereinsvorsitzende ein Schreiben der Stadt an ihn zukommen, wonach die Überprüfung – verkürzt gesagt – im Zusammenhang mit der Überwachung von Ausländervereinen gestanden habe. Da das Baskenland ein „politisch sensibler Bereich“ sei, sei es angezeigt, den Verein gelegentlich auf politische Hintergründe zu überprüfen. Für diese präventive Maßnahme der Sicherheitsbehörden werde vor dem Hintergrund der jüngsten terroristischen Anschläge innerhalb und außerhalb Europas um Verständnis gebeten.

Hinsichtlich unserer Fragen nach der generellen Verfahrensweise im Lande teilte uns das Innenministerium mit, dass die Gesamtzahl der aufgrund des Erlasses überprüften Vereine nicht bekannt sei, da nur die als „relevant erkannten“ Vereine erfasst würden. Gespeichert worden seien im Wesentlichen als extremistisch eingestufte Vereine (in der Regel im Verfassungsschutzbericht des Landes genannt), Vereine mit engen Verbindungen zu einer verbotenen Vereinigung oder solche Vereine, in deren Räumen mutmaßlich zu Straftaten aufgerufen wird oder

bei denen potenzielle Straftäter verkehren bzw. aktiv sind. Die relevanten Vereine (derzeit 19 in Baden-Württemberg) seien in der Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK, vgl. 2. Teil, 1. Abschnitt, Nr. 4 dieses Tätigkeitsberichts) gespeichert worden.

Was den konkreten Fall anging, so ließ uns das Innenministerium nach nochmaliger Abklärung mit dem Landeskriminalamt einige Zeit später wissen, dass die Hintergründe der damaligen Befragung weiterhin unklar seien. Zwar komme grundsätzlich § 20 Abs. 1 Satz 1 PolG als Rechtsgrundlage für polizeiliche Befragungen in Betracht; der von der Polizeidirektion mitgeteilte Sachverhalt habe aber für das Vorliegen einer konkreten Gefahr keine ausreichenden Anhaltspunkte ergeben. In einem Erlass an die Polizeidirektion stellte das Innenministerium zudem klar, dass die Stadt als Kreispolizeibehörde im Zusammenhang mit der Anmeldepflicht von Ausländervereinen zwar um Auskünfte ersuchen könne, dass die ersuchte Stelle aber grundsätzlich (nur) zur Übermittlung bereits vorhandener Daten, nicht jedoch zur (erstmaligen) Datenerhebung zum Zweck der Beantwortung des Auskunftsersuchens berechtigt sei. Soweit die Polizeidirektion daneben von sich aus eine Befragung durchführen wollte, müsse dies zur Wahrnehmung einer konkreten polizeilichen Aufgabe aus einem bestimmten Anlass erforderlich sein. Eine Befragung „ins Blaue hinein“ oder eine allgemeine Ausforschung sei auch nach § 20 Abs. 1 PolG nicht zulässig. Die von der Polizeidirektion offenbar ins Feld geführte „allgemeine polizeiliche Erfahrung, dass das Vereinsrecht in Einzelfällen gesetzeswidrig missbraucht wird“, ließ das Innenministerium nicht gelten. Es hätten nämlich keinerlei Anhaltspunkte dafür vorgelegen, dass von dem Verein eine Gefahr für die öffentliche Sicherheit oder Ordnung ausgehe.

Die geschilderte Überprüfungsaktion der Polizei, bei der auch die Stadt keine rühmliche Rolle spielte, hat sich demnach in Wohlgefallen aufgelöst. Es bleibt zu hoffen, dass es sich um einen einmaligen Ausrutscher gehandelt hat. Das Innenministerium hat den Polizeidienststellen jedenfalls mit der wünschenswerten Deutlichkeit ins Stammbuch geschrieben, dass Vereine, auch wenn sie einen Auslandsbezug aufweisen, nicht unter Generalverdacht gestellt werden dürfen. Beschwerden anderer Vereine sind bei uns bisher nicht eingegangen.

8.2 Wieder mal zu lange gespeichert – die Aussonderungsprüffristen im Zusammenhang mit Sexualdelikten

Wer in Verdacht steht, eine Straftat begangen zu haben, wird von der Polizei in den einschlägigen Dateien gespeichert, sofern die Polizei eine Wiederholungsgefahr bejaht. In Baden-Württemberg erfolgt die Datenspeicherung im Polizeilichen Auskunftssystem Baden-Württemberg (POLAS-BW), auf Bundesebene in der beim Bundeskriminalamt geführten Verbunddatei von Bund und Ländern (INPOL-Z). Für Sexualdelikte gelten teilweise überdurchschnittlich lange Speicherfristen von bis zu 20 Jahren, allerdings hängt die konkrete Speicherdauer vom konkreten Tatvorwurf ab. Dass es offenbar nicht immer leicht fällt, hier den Überblick zu behalten, haben wir mehr durch Zufall erfahren, als wir der Beschwerde eines Mannes aus dem Rems-Murr-Kreis nachgingen. Eigentlich wollte er vor allem wissen, wie bestimmte Informationen aus einer Wohnungsdurchsuchung an die Fahrerlaubnisbehörde gelangt waren, was in der Folge zur Entziehung der Fahrerlaubnis geführt hatte. Als wir bei der Polizei nachfragten, wie sich die Sache abgespielt hat, wollten wir auch wissen, welche Daten über den Petenten gespeichert worden sind. Daraufhin wurde uns mitgeteilt, dass der Betroffene wegen eines Sexualdelikts nach § 184 b Abs. 3 des Strafgesetzbuchs (StGB) für die Dauer von 20 Jahren in POLAS-BW eingespeichert worden sei; dieser Paragraph bezieht sich auf die Verbreitung, den Erwerb und den Besitz kinderpornographischer Schriften. Nun sieht zwar § 38 Abs. 2 des Polizeigesetzes (PolG), in dem die maximalen Speicherfristen geregelt sind, vor, dass die Speicherdauer bei einer Sexualstraftat nach dem 13. Abschnitt des Strafgesetzbuchs 20 Jahre betragen darf; der 13. Abschnitt umfasst sämtliche Straftaten gegen die sexuelle Selbstbestimmung. Jedoch regelt § 38 Abs. 2 Satz 3 Nr. 1 PolG zu-

gleich, dass Straftaten nach den §§ 183 a, 184, 184 a und 184 b StGB von der 20-jährigen Speicherfrist ausgenommen sind.

Im Fall des Mannes aus dem Rems-Murr-Kreis hätte demnach „nur“ eine maximal zehnjährige Speicherdauer festgesetzt werden dürfen. Warum dies nicht erfolgte, ließ sich nicht mehr genau klären. Die Polizeidirektion Waiblingen berief sich zwar zunächst auf angebliche Weisungen des Landeskriminalamts oder des Innenministeriums. Möglicherweise war hiermit die „Führungs- und Einsatzanordnung zur intensivierten Bekämpfung von Sexualstraftaten“ aus dem Jahre 2001 gemeint, die wir schon in unserem 22. Tätigkeitsbericht (LT-Drucksache 13/520) kritisch kommentiert hatten. Seinerzeit hatte das Innenministerium die Aussonderungsprüffristen für „einfache“ Sexualstraftaten bei Erwachsenen auf zehn Jahre und bei Jugendlichen auf fünf Jahre angehoben und außerdem vorgegeben, dass die 20-jährige Prüffrist „regelmäßig ausgeschöpft“ werden solle. Es war aber keine Rede davon gewesen, dass die in § 38 Abs. 2 Satz 3 Nr. 1 PolG genannten Ausnahmen nicht mehr gelten sollten. Das um Stellungnahme gebetene Innenministerium bestätigte denn auch, dass die genannten Ausnahmen von der 20-jährigen Speicherfrist weiter gelten würden; eine generelle Heraufsetzung von Prüffristen außerhalb des § 38 PolG gebe es nicht.

Dass es sich hier aber nicht um einen Einzelfehler handelte, ergab eine aufgrund unserer Nachfrage durch das Landeskriminalamt veranlasste Auswertung in POLAS-BW. Dabei wurde festgestellt, dass landesweit 285 Datensätze mit den Ausnahmedelikten nach §§ 183 a, 184, 184 a und 184 b StGB eingespeichert waren, die eine Laufzeit von über zehn Jahren aufwiesen. Das Innenministerium stimmte mit uns erfreulicherweise darin überein, dass eine rasche Korrektur der Datensätze erforderlich war. Das Landeskriminalamt forderte deshalb die betroffenen Polizeidienststellen auf, die fraglichen Datensätze kritisch zu prüfen und die Prüffristen entsprechend zu korrigieren. Auch im Falle des Mannes aus dem Rems-Murr-Kreis geschah dies: Die Aussonderungsprüffrist wurde auf ein Datum im Jahr 2012 (zehn Jahre nach der letzten Tat) verkürzt. Generell bleibt zu hoffen, dass die Fristen auch in den übrigen Fällen angepasst wurden und dass bei der Vergabe von Aussonderungsprüffristen künftig genauer hingeschaut wird.

## 2. Abschnitt: Die Justiz

### 1. Datenschutzkontrolle bei Gerichten

Der regelmäßige Leser unseres Tätigkeitsberichts weiß, dass das Thema „Datenschutzkontrolle bei den Gerichten“ über Jahre in jedem unserer Tätigkeitsberichte vertreten war (vgl. 20. Tätigkeitsbericht, LT-Drucksache 12/4600; 21. Tätigkeitsbericht, LT-Drucksache 12/5740; 22. Tätigkeitsbericht, LT-Drucksache 13/520; 23. Tätigkeitsbericht, LT-Drucksache 13/1500). Wegen der im Grundgesetz garantierten Unabhängigkeit der Richter ist die Kontrollkompetenz unserer Dienststelle bei Gerichten stark eingeschränkt, was aber nichts daran ändert, dass die Gerichte des Landes datenschutzrechtliche Vorschriften inhaltlich beachten müssen. In § 2 Abs. 3 LDSG ist geregelt, dass unsere Dienststelle Gerichte nur kontrollieren darf, soweit diese in Verwaltungsangelegenheiten tätig sind. Die Frage, in welchen Fällen eine Verwaltungsangelegenheit vorliegt, wurde vom Justizministerium jedoch jahrelang völlig anders beurteilt als von uns. Unsere Dienststelle vertrat stets die Auffassung, dass sich die Prüfung, ob Gerichte beim Einsatz der EDV die nach § 9 LDSG gebotenen technischen und organisatorischen Maßnahmen getroffen haben, auf Verwaltungsangelegenheiten bezieht und weder die richterliche Datenverarbeitung noch die richterliche Arbeitsweise am Fall betrifft. Das Justizministerium vertrat dagegen lange Zeit die Ansicht, die Rechtspflege, und damit auch der Einsatz der EDV-Technik, sei umfassend von der Kontrolle unserer Dienststelle ausgenommen. Dies hatte zur Folge, dass das Justizministerium in den Jahren 1999 und 2000 von unserer Dienststelle bei Gerichten vorgesehene Kontrollen der dort eingesetzten EDV verhindert hat. Schließlich gelang es jedoch, das Justizministerium davon zu überzeugen, dass sich typische Fragen des technischen und orga-

nisatorischen Datenschutzes prüfen lassen, ohne dabei die richterliche Datenverarbeitung zu tangieren. Auch über den Umfang der unserer Dienststelle zustehenden Kontrollbefugnisse konnte mit dem Justizministerium weitgehend Übereinstimmung erzielt werden. Nach einigem weiteren Hin und Her konnten wir dann Anfang dieses Jahres einen Kontrollbesuch bei einem Gericht durchführen. Um noch einmal klarzustellen, dass von unserer Seite in keiner Weise beabsichtigt war, die Tätigkeit der Richter zu überprüfen, haben wir im Vorfeld zusammen mit dem Justizministerium und dem von uns ausgewählten Gericht den Umfang der Kontrolle genau festgelegt. Wir hoffen, etwaige Zweifel daran, dass eine datenschutzrechtliche Kontrolle bei Gerichten ohne Eingriff in die richterliche Tätigkeit möglich ist, durch diesen Kontrollbesuch endgültig ausgeräumt zu haben.

Auch gegenüber Bürgern, die sich mit Eingaben an uns wenden, ist die eingeschränkte Kontrollkompetenz unserer Dienststelle bei Gerichten ein regelmäßig wiederkehrendes Thema. So wenden sich jedes Jahr Bürger an uns, weil sie der Meinung sind, ein Richter habe sie im Rahmen eines Gerichtsverfahrens, z. B. durch die Beweiswürdigung, durch ein Urteil oder eine sonstige richterliche Entscheidung, in ihrem Recht auf informationelle Selbstbestimmung verletzt. In diesen Fällen können wir nichts anderes tun, als die Betroffenen darauf hinzuweisen, dass wir ihren konkreten Einzelfall – mangels Zuständigkeit – nicht überprüfen können.

Trotz richterlicher Unabhängigkeit wenden wir uns jedoch von Zeit zu Zeit auch in gerichtlichen Angelegenheiten, die sich nicht auf Verwaltungsangelegenheiten beziehen, an das Justizministerium oder die Gerichte. So kommt es z. B. vor, dass wir – unter Hinweis auf unsere Unzuständigkeit – darum bitten, bestimmte datenschutzrechtliche Vorgehensweisen zu überdenken, oder Vorschläge machen, wie datenschutzrechtliche Aspekte stärker berücksichtigt werden könnten.

### 1.1 Kontrollbesuch beim Verwaltungsgericht

Die zwischen dem Justizministerium und unserer Dienststelle vereinbarten Grundsätze für die Durchführung von Datenschutzkontrollen an Gerichten hatten in diesem Jahr ihre erste Bewährungsprobe zu bestehen, als wir eine Kontrolle an einem Verwaltungsgericht durchführten.

Inhaltlich stand dabei die Überprüfung der Zugriffsberechtigungen im Mittelpunkt. Den besonderen Bedingungen für eine Datenschutzkontrolle bei Gericht ist es zuzuschreiben, dass wir dabei nicht – wie dies ansonsten üblich ist – der Frage nachgegangen sind, ob die in den überprüften Dokumenten enthaltenen personenbezogenen Daten für die Aufgabenerfüllung des Verwaltungsgerichts überhaupt erforderlich sind. Gegenstand unserer Kontrolle war stattdessen lediglich, ob die vom Gericht selbst zu erstellenden Vorgaben dafür, wer auf welche Dokumente Zugriff erhalten darf, bei der Einrichtung der im Computersystem hinterlegten und für jeden Zugriff benötigten Zugriffsberechtigungen berücksichtigt wurden. Dem lag die sowohl vom Justizministerium als auch von uns vertretene Auffassung zugrunde, dass auch Gerichte für ihren Dienstbetrieb interne Regelungen aufstellen müssen, aus denen hervorgeht, welche Bediensteten Zugriff auf welche elektronisch gespeicherten Daten benötigen.

In seinem Bürokommunikationssystem hatte das Gericht etliche elektronische Ablagen eingerichtet. Beispielsweise gab es – korrespondierend zur Anzahl der Kammern des Gerichts – Ablagen mit Bezeichnungen wie „Kammer01“, „Kammer02“, ... . Für diese Unterordner waren jeweils Zugriffsberechtigungen für bestimmte Benutzergruppen eingerichtet. Obwohl die Nutzer des Verwaltungsgerichts dazu in ca. 50 Benutzergruppen zusammengefasst waren, hatte das Verwaltungsgericht keine schriftliche Konzeption dafür erstellt, welche Benutzer und welche Benutzergruppen auf welche dieser Ablagen zugreifen dürfen. Nach den Ausführungen der Vertreter des Verwaltungsgerichts könne auf ein solches schriftliches Konzept auch ohne weiteres verzichtet werden, da sich bereits aus der Bezeichnung der Ordner eindeutig ergebe, welche Bediensteten darauf jeweils zugreifen können müssen. Hinsicht-

lich der „Kammer“-Ordner ergäben sich die Zugriffsberechtigungen beispielsweise aus der gerichtlichen Organisationsstruktur. Die Richter zweier Kammern, die aus je einem Vorsitzenden Richter sowie fünf oder sechs Richtern zusammengesetzt seien, bildeten gemeinsam mit jeweils zwei Urkundsbeamten sowie einer oder zwei Schreibkräften eine so genannte Serviceeinheit, wobei die Urkundsbeamten sowie die Schreibkräfte für die Richter beider Kammern tätig würden. Darauf abgestimmt seien die Zugriffsberechtigungen so eingerichtet, dass die Richter jeweils nur auf die elektronische Ablage der Kammer zugreifen können, deren Mitglied sie seien. Die Urkundsbeamten und Schreibkräfte hingegen könnten auf beide, der Serviceeinheit zugeordneten Kammerordner zugreifen. Um auf besondere Aufgabenschwerpunkte in einzelnen Kammern flexibel reagieren zu können, gebe es darüber hinaus noch vier Schreibkräfte, die auf alle Kammerordner zugreifen könnten.

Beim Vergleich dieses mündlich erläuterten Sollkonzepts mit den tatsächlich eingerichteten Zugriffsberechtigungen stellte sich jedoch heraus, dass diese von dem Sollkonzept deutlich abwichen. Die tatsächlich eingerichteten Zugriffsberechtigungen basierten nämlich nicht auf dem zuvor beschriebenen Modell der Servicestellen, sondern ließen zu, dass sämtliche Urkundsbeamte und sämtliche Schreibkräfte des Verwaltungsgerichts auf alle Kammerablagen zugreifen konnten. Auch hinsichtlich anderer Ablagen waren umfangreichere Berechtigungen im System hinterlegt, als dies nach den Erläuterungen des Gerichts hätte sein sollen.

Wir teilten dem Verwaltungsgericht mit, dass wir die im Vergleich zum Sollkonzept zu umfangreich gewährten Zugriffsberechtigungen als datenschutzrechtlichen Mangel ansehen. Unserer Aufforderung entsprechend erstellte das Gericht daraufhin ein schriftliches Konzept für die Einrichtung der Zugriffsberechtigungen und sorgte dafür, dass die tatsächlich eingerichteten Zugriffsberechtigungen diesem Konzept entsprechen. Zudem stellte es in Aussicht, die Übereinstimmung des Ist-Zustands mit dem Sollkonzept auch künftig regelmäßig zu überprüfen und zudem verstärkt darauf zu achten, dass nicht mehr benötigte Zugriffsberechtigungen zeitnah gelöscht werden.

1.2 Überprüfung richterlicher Durchsuchungsbeschlüsse

Im Laufe des Berichtsjahrs haben uns mehrere Petenten gebeten zu prüfen, ob bei ihnen im Rahmen von strafrechtlichen Ermittlungsverfahren durchgeführte Wohnungsdurchsuchungen rechtmäßig erfolgt sind. Da diese Durchsuchungen jeweils aufgrund richterlicher Durchsuchungsbeschlüsse durchgeführt wurden, konnten wir diesen Bitten nur teilweise nachkommen. Die Frage, ob die richterlichen Durchsuchungsbeschlüsse zu Recht ergangen sind oder ob ihr Inhalt, z. B. bezüglich der zu durchsuchenden Räumlichkeiten, rechtmäßig ist, liegt – wegen der grundgesetzlich garantierten Unabhängigkeit der Richter – außerhalb der Zuständigkeit unserer Dienststelle. In derartigen Fällen beschränkt sich unsere Prüfung daher auf die konkrete Vorgehensweise der die Durchsuchung durchführenden Beamten. Wir prüfen lediglich, ob die Beamten sich an den vom Richter im Durchsuchungsbeschluss festgelegten Umfang der Durchsuchung gehalten haben, also ob das Vorgehen der Beamten vom richterlichen Beschluss gedeckt ist.

1.3 Bekanntmachung des Zwangsversteigerungstermins

Geraten Haus- und Grundbesitzer in wirtschaftliche Schwierigkeiten, kann es zur Zwangsversteigerung des Grundstücks kommen. Wann wo welches Grundstück oder welche Eigentumswohnung zwangsversteigert werden soll, ist in den öffentlichen Bekanntmachungen der Vollstreckungsgerichte über anstehende Zwangsversteigerungen nachzulesen. Bis vor einiger Zeit sah § 38 des Zwangsversteigerungsgesetzes (ZVG) vor, dass die Terminsbestimmung auch Angaben über den Eigentümer enthalten soll (nicht muss!), weshalb den öffentlichen Bekanntmachungen oftmals zu entnehmen war, wie der Eigentümer heißt

und in welchem Ort er wohnt. Unsere Dienststelle hatte gegenüber dem Justizministerium schon vor Jahren die Auffassung vertreten, dass die Nennung persönlicher Daten des Eigentümers in der Terminsbestimmung in der Praxis ihre Bedeutung verloren hat, da es äußerst selten vorkommen dürfte, dass ein bis dahin unbekannter Berechtigter durch die Veröffentlichung des Zwangsversteigerungstermins mit Benennung des Eigentümers aufgespürt wird (vgl. 10. Tätigkeitsbericht, LT-Drucksache 10/2730). Unsere Zweifel an der Verhältnismäßigkeit der Veröffentlichung persönlicher Daten des Eigentümers, die diesen ganz erheblich beeinträchtigen und in seiner sozialen Geltung herabwürdigen kann, hat das Justizministerium damals zwar nicht geteilt. Es hat jedoch die Vollstreckungsgerichte über unsere Auffassung unterrichtet. Und tatsächlich haben in den folgenden Jahren immer mehr Vollstreckungsgerichte das durch § 38 ZVG eingeräumte Ermessen voll ausgeschöpft und in Fällen, in denen keine Anhaltspunkte für das Bestehen unbekannter Rechte gegeben waren, auf die Namensnennung des Eigentümers verzichtet.

Durch das Erste Justizmodernisierungsgesetz vom 24. August 2004 (BGBl. I 2004, S. 2198) ist § 38 ZVG schließlich doch geändert worden. Angaben zum Eigentümer sind nicht mehr vorgesehen. Die entsprechende Passage des § 38 ZVG ist ersatzlos gestrichen worden. In der Begründung zum damaligen Gesetzentwurf ist hierzu ausgeführt, dass die Namensnennung in der Terminsbestimmung nicht mehr den Anforderungen des heutigen Datenschutzes entspricht. Wir gingen davon aus, dass das Thema damit ein für alle Mal erledigt ist. Umso erstaunter waren wir, als wir im Frühjahr 2006 feststellten, dass ein Vollstreckungsgericht trotz Änderung des § 38 ZVG in der Terminsbestimmung nach wie vor regelmäßig Angaben zum Eigentümer machte. Obwohl sich diese Angelegenheit nicht auf eine Verwaltungstätigkeit im Sinne des § 2 Abs. 3 LDSG bezog, haben wir das Vollstreckungsgericht auf die geänderte Rechtslage aufmerksam gemacht und gebeten, künftig entsprechend zu verfahren. Das Vollstreckungsgericht ist dieser Bitte nachgekommen. Kurze Zeit später konnten wir feststellen, dass die öffentlichen Bekanntmachungen der Zwangsversteigerungstermine dieses Gerichts keine Angaben zum Eigentümer mehr enthielten.

**2. Entwurf eines Gesetzes zur Aufbewahrung von Schriftgut der Justiz**

Im Bereich der Justiz werden in großem Umfang Daten erhoben und auch nach Abschluss des jeweiligen Verfahrens noch jahrelang gespeichert. Obwohl das Bundesverfassungsgericht bereits im Volkszählungsurteil aus dem Jahr 1983 darauf hingewiesen hat, dass die Erhebung und Speicherung personenbezogener Daten einer gesetzlichen Grundlage bedarf, aus der sich die Voraussetzungen und der Umfang derartiger Eingriffe in das Recht des Einzelnen auf informationelle Selbstbestimmung klar und für den Bürger erkennbar ergeben, existieren für die Aufbewahrung, Aussonderung und Vernichtung des Schriftguts der Justizbehörden der Länder nach wie vor keine bereichsspezifischen gesetzlichen Regelungen. Und auch für das Schriftgut der Bundesjustizbehörden fehlte es bis vor kurzem an einer den Vorgaben des Volkszählungsurteils entsprechenden gesetzlichen Grundlage. Das Gesetz zur Aufbewahrung von Schriftgut der Gerichte des Bundes und des Generalbundesanwalts nach Beendigung des Verfahrens (Schriftgutaufbewahrungsgesetz, BGBl. 2005, Seite 852) trat erst am 1. April 2006, also mehr als 20 Jahre nach dem Volkszählungsurteil, in Kraft.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher bereits seit vielen Jahren in mehreren Entschließungen darauf hingewiesen, dass die Aufbewahrung, Aussonderung und Vernichtung von Akten bei der Justiz einer bereichsspezifischen gesetzlichen Regelung bedarf. Auf Drängen der Datenschutzbeauftragten haben die Justizministerinnen und Justizminister schließlich auf ihrer 72. Konferenz vom 11. bis 13. Juni 2001 die Einsetzung einer Arbeitsgruppe beschlossen, die den Entwurf eines Aktenaufbewahrungsgesetzes erarbeiten sollte. In diesem sollten die grundsätzlichen Voraussetzungen für die Aufbewahrung des Schriftguts festgelegt und die Länder ermächtigt werden, die Einzelheiten, also die konkreten Fristen, in (bundeseinheitlich) abgestimmten Rechtsverordnungen oder

Verwaltungsvorschriften zu regeln. Trotz dieses Beschlusses ist zunächst nichts geschehen, weshalb die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. und 25. Oktober 2002 in einem Beschluss die unverzügliche Schaffung eines Aktenaufbewahrungsgesetzes gefordert hat.

Immerhin ist – wie bereits erwähnt – zum 1. April 2006 für die Gerichte des Bundes und den Generalbundesanwalt das Schriftgutaufbewahrungsgesetz in Kraft getreten. Und schließlich wurde unserer Dienststelle im September 2006 der sich auf die Landesjustizbehörden beziehende Entwurf eines Gesetzes zur Aufbewahrung von Schriftgut der ordentlichen Gerichtsbarkeit, der Fachgerichtsbarkeiten, der Staatsanwaltschaften und der Justizvollzugsbehörden vorgelegt, der sich eng am Schriftgutaufbewahrungsgesetz für die Gerichte des Bundes und des Generalbundesanwalts orientiert. Im Hinblick auf die Vorgaben des Volkszählungsurteils und die mit der Aktenaufbewahrung verbundenen Eingriffe in die informationelle Selbstbestimmung hoffen wir, dass die Angelegenheit nun zügig zum Abschluss gebracht wird.

### 3. Recherchetätigkeit der Justiz für den SWR

Es steht außer Frage, dass Gerichte aufgrund verfassungsrechtlicher Grundsätze – wie etwa zur Fortbildung des Rechts oder um dem Bürger die Möglichkeit zu geben, in Erfahrung bringen zu können, welche Rechte er hat und welche Pflichten ihm obliegen – verpflichtet sind, veröffentlichungswürdige Entscheidungen unter Wahrung der Rechte der Betroffenen weiterzugeben bzw. die Öffentlichkeit durch Unterrichtung der Medien über laufende Verfahren zu informieren. Nicht unter die genannten Kategorien fällt folgender Fall, der im Mai des Berichtsjahrs für Schlagzeilen sorgte.

Für eine Sendung mit dem Titel „Die Macht der Sterne“ suchte die Redaktion des SWR-Nachtcafés nach Personen, die „Opfer“ von Astrologen geworden waren. Auf eine entsprechende Anfrage des SWR hatte das Justizministerium per Rundmail alle Gerichte und Staatsanwaltschaften aufgefordert, das SWR-Nachtcafé bei der Suche nach „Geschädigten, Opfern oder Prozessbeteiligten, die auf den Rat von Astrologen hereingefallen sind“, zu unterstützen. Dem Justizministerium ging es hierbei nicht darum, dem SWR Namen, Anschriften oder Verhaltensweisen von Betroffenen mitzuteilen. Geplant war vielmehr eine Kontaktvermittlung durch Weiterleitung der entsprechenden SWR-Anfrage an die Betroffenen. Eine derartige Weiterleitung hätte entweder durch das Justizministerium selbst oder aber durch das jeweilige Gericht oder die Staatsanwaltschaft erfolgen sollen, verbunden mit dem Hinweis, dass es die freie Entscheidung jedes Einzelnen sei, dann von sich aus Kontakt mit dem SWR aufzunehmen oder die Anfrage zu ignorieren. Obwohl die Aufforderung des Justizministeriums letztendlich weder zu einer Übermittlung personenbezogener Daten Betroffener an den SWR noch zu einer Kontaktvermittlung in der vorgenannten Art oder zu einer Übermittlung personenbezogener Daten von den Gerichten und Staatsanwaltschaften an das Justizministerium geführt hat, haben wir die Vorgehensweise des Justizministeriums – nicht zuletzt im Hinblick auf mögliche künftige Fälle – einer datenschutzrechtlichen Prüfung unterzogen. Diese hat Folgendes ergeben:

Die schon erwähnte E-Mail des Justizministeriums war aus datenschutzrechtlicher Sicht bereits deshalb problematisch, weil ihr nicht eindeutig zu entnehmen war, dass dem SWR keine personenbezogenen Daten übermittelt werden sollten. Die E-Mail hatte dies vielmehr völlig offen gelassen. Aber auch die geplante Kontaktvermittlung war datenschutzrechtlich nicht unbedenklich. Die vom Justizministerium als möglich angesehene Zuleitung der SWR-Anfrage an einen Betroffenen durch das Justizministerium hätte die Übermittlung personenbezogener Verfahrensdaten durch ein Gericht oder eine Staatsanwaltschaft an das Justizministerium und die entsprechende Erhebung dieser Daten durch das Justizministerium vorausgesetzt. Auch die Vorgehensweise, dass das jeweilige Gericht oder die Staatsanwaltschaft selbst die Anfrage des SWR an einen Betroffenen weiterleitet, ist datenschutzrechtlich nicht unerheblich. Denn die Nutzung von Verfahrensdaten zum Zwecke der Weiterleitung der SWR-Anfrage an einen Be-

troffenen durch einen Richter oder Staatsanwalt hätte ebenfalls eine Verarbeitung personenbezogener Daten dargestellt. Einziger Zweck derartiger Maßnahmen wäre gewesen, einen Sender bei der Suche nach potenziellen Gästen für eine Talkshow zu unterstützen. Die vorgesehene Kontaktvermittlung war somit nicht auf die Übermittlung von Fakten zu einem bestimmten Tatsachenkomplex gerichtet. Vorausgegangen war auch nicht eine Anfrage des SWR zu einem konkreten Verfahren. Angestrebt war vielmehr eine bloße Recherchetätigkeit und Adressmittlung der Justiz für den SWR. Dass eine zu diesem Zweck vorgenommene Datenverarbeitung von der im Landespressegesetz geregelten Auskunftspflicht der Behörden der Presse, dem Rundfunk und dem Fernsehen gegenüber gedeckt ist, halten wir für äußerst zweifelhaft. Andere Rechtsgrundlagen, auf die derartige Datenverarbeitungsvorgänge hätten gestützt werden können, sind ebenfalls nicht ersichtlich.

Die Aufforderung des Justizministeriums, den SWR zu unterstützen, hat zwar letztendlich nicht zu Datenschutzverletzungen geführt. Dennoch haben wir das Justizministerium gebeten, künftig sicherzustellen, dass bei der Öffentlichkeitsarbeit die datenschutzrechtlichen Anforderungen beachtet werden. Im Ergebnis dürfte dies bedeuten, dass die Übernahme einer allgemeinen Recherchetätigkeit für anfragende Stellen grundsätzlich nicht in Betracht kommt.

### 4. Beteiligung von Interessenverbänden an Strafermittlungen

Im Rahmen von strafrechtlichen Ermittlungsverfahren wegen Urheberrechtsverletzungen können Computer, Festplatten, Datenträger, Videobänder u. Ä. sichergestellt werden. Um den Verdacht zu überprüfen, ob diese Mittel oder Ergebnis von Urheberrechtsverletzungen sind, ist eine Auswertung der sichergestellten Datenträger vorzunehmen. Im Laufe des Berichtsjahrs wurden wir darüber informiert, dass für derartige Auswertungen deutschlandweit zunehmend eine Organisation der Film-, Software- und Entertainmentbranche und ihrer Verbände als externe Sachverständige eingesetzt wird, die sich satzungsgemäß die Ermittlung und Verfolgung von Fällen der sog. Produktpiraterie zur Aufgabe gemacht hat. Um in Erfahrung zu bringen, ob dieser Organisation auch personenbezogene Daten übermittelt werden, und im Hinblick auf die von Sachverständigen zu fordernde Neutralität baten wir das Justizministerium um Stellungnahme.

Das Justizministerium bestätigte, dass die Organisation auch von Staatsanwaltschaften in Baden-Württemberg in einschlägigen Ermittlungsverfahren beteiligt werde. Die Mehrzahl der Staatsanwaltschaften würde die Organisation zur Klärung der Frage heranziehen, ob die auf sichergestellten Datenträgern gespeicherten Werke urheberrechtlich geschützt sind und wer insoweit Rechteinhaber ist. Zu diesem Zweck seien der Organisation bislang überwiegend Auflistungen der sichergestellten Werke oder aber die sichergestellten CDs, DVDs usw. übersandt worden. In wenigen Ausnahmefällen seien der Organisation allerdings auch schon komplette Festplatten zur Auswertung übergeben worden.

Das Justizministerium ist wie wir der Ansicht, dass eine Sachverständigentätigkeit der Organisation bzw. ihrer Mitarbeiter im Hinblick auf das Erfordernis der Neutralität von Sachverständigen nicht in Betracht kommt. Gestützt wird diese Ansicht durch eine Entscheidung des Landgerichts Kiel vom 14. August 2006 (Az: 37 Qs 54/06). In dieser kommt das Landgericht zu dem Ergebnis, dass sich bereits aus der Zielsetzung der Organisation ergebe, dass ihren Mitarbeitern die von einem Sachverständigen zu fordernde Neutralität fehle. Bei den oben angesprochenen Tätigkeiten der besagten Organisation handle es sich – so das Justizministerium – jedoch ganz überwiegend nicht um Tätigkeiten eines Sachverständigen im Sinne der Strafprozessordnung. Zentrales Charakteristikum des Sachverständigen sei die besondere Sachkunde, die dieser entweder dem Gericht bzw. der Staatsanwaltschaft vermittelt oder aufgrund derer er in der Lage ist, bestimmte Feststellungen zu treffen, die ein Laie nicht treffen kann. Soweit die Organisation lediglich von der Polizei erstellte Listen oder die sichergestellten CDs und DVDs auf urheberrechtlich relevante Werke hin durchsieht, fehle es insoweit an einem Tätigwerden aufgrund besonderer Sachkunde. Die „Sach-

kunde“ der Organisation bestehe in diesen Fällen ausschließlich darin, dass sie über ein aktuelles Verzeichnis der urheberrechtlich geschützten Werke verfüge, mit dem sie die Liste bzw. die sichergestellten Werke vergleichen kann. Würde man das entsprechende Verzeichnis der Polizei zur Verfügung stellen, wäre diese ohne weiteres in der Lage, den Abgleich selbst vorzunehmen. Problematisch wäre insoweit allenfalls die Sicherstellung der Aktualität des Verzeichnisses. Das Justizministerium vergleicht diese Tätigkeit der Organisation mit dem Abgleich etwa sichergestellter Geldscheine mit registrierten Nummern aus einem Raub oder einer Erpressung oder mit der Vorlage sichergestellten Diebesguts an einen Geschädigten zum Zweck der Identifizierung. Soweit die Organisation nur in dem genannten Umfang tätig werde, liege eine bloße Auskunftserteilung vor, der das Neutralitätserfordernis nicht entgegenstehe. Eine unzulässige Sachverständigentätigkeit liege dagegen vor, wenn die Organisation zusätzlich Umstände feststellen soll, die besondere Sachkunde auf EDV-technischem Gebiet erfordern. Das Justizministerium nennt hierfür als Beispiel die Auswertung einer Festplatte zur Ermittlung der Herkunft oder einer etwaigen Weiterverteilung der Werke.

Die Übersendung von Auflistungen der sichergestellten Werke oder die Übersendung von sichergestellten CDs, DVDs usw. an die Organisation, auf denen außer den möglicherweise urheberrechtsrelevanten Werken keine weiteren Daten gespeichert sind, ist nach Ansicht des Justizministeriums aus datenschutzrechtlicher Sicht unproblematisch. Da es in der Praxis jedoch kaum vorkommen dürfte, dass auf Festplatten bzw. Rechnern keine über die verfahrensrelevanten Werke hinausgehenden personenbezogenen Daten gespeichert sind, hält das Justizministerium die Übersendung kompletter Festplatten an die Organisation dagegen für datenschutzrechtlich bedenklich.

Mit den Staatsanwaltschaften hat sich das Justizministerium zwischenzeitlich dahin gehend verständigt, dass eine Beauftragung der Organisation bzw. ihrer Mitarbeiter als Sachverständige nicht in Betracht kommt, eine Übersendung von Festplatten nicht erfolgen darf und ansonsten nur solche Datenträger übergeben werden dürfen, die über die möglicherweise urheberrechtlich relevanten Werke hinaus keine Daten enthalten.

Soweit der Organisation tatsächlich nur solche Datenträger übergeben werden, die keine personenbezogenen Daten enthalten, stimmen wir dem Justizministerium darin zu, dass es datenschutzrechtlich unbedenklich ist, wenn die Organisation zur Klärung der Frage herangezogen wird, ob die auf sichergestellten Datenträgern gespeicherten Werke urheberrechtlich geschützt sind und wer insoweit Rechteinhaber ist.

## 3. Teil: Gesundheit und Soziales

Im Jahr der Fußballweltmeisterschaft gab es kein Thema, das neben diesem sportlichen Topereignis in der Medienöffentlichkeit und auch von den Bürgern vergleichbar intensiv und kontrovers diskutiert wurde, wie dies bei der Gesundheitsreform der Fall war und wohl auch weiterhin bleiben wird. Kein Wunder: Sind von diesem Reformvorhaben, das Elemente der Kopfpauschale und solche der Bürgerversicherung unter einem Reformdach zu vereinen versucht und dabei noch die Finanzierung der Gesetzlichen Krankenversicherung durch die Schaffung eines Gesundheitsfonds auf eine stabilere Grundlage stellen möchte, ca. 70 Millionen gesetzlich Versicherte unmittelbar finanziell betroffen.

Nach zähem Ringen um den richtigen Weg für einen Umbau dieses Teils unseres Sozialversicherungssystems hat die Große Koalition Anfang Juli 2006 die Eckpunkte für eine Gesundheitsreform beschlossen. Nach dieser Einigung, bei der zum Teil nur auf Überschriftenebene ein Konsens erzielt werden konnte, wurde die Diskussion um deren inhaltliche Ausgestaltung nur noch heftiger und auch im Ton deutlich schärfer, was schließlich zu einer Verschiebung des geplanten Starts auf den 1. April 2007 führte. Anfang Oktober 2006 wurde schließlich ein weiterer Kompromiss dahin gehend erzielt, wichtige Teile des Reformpakets wie z. B. den Gesundheitsfonds und den Finanzausgleich der Krankenkassen in das Jahr 2009 zu verschieben. Inzwischen befindet sich der über 500-seitige Regierungsentwurf im parlamentarischen Beratungsverfahren.

Auch diese Entwicklung kann nicht wirklich verwundern, geht es im Gesundheitswesen doch um sehr viel Geld, allein um über 28 Milliarden Euro pro Jahr im Südwesten. Es gibt dazu eine Vielzahl von Akteuren mit sehr unterschiedlichen Interessenlagen. So arbeiten in Baden-Württemberg rd. 12 % aller Erwerbstätigen im Gesundheitswesen, das heißt, dass etwa 580 000 Arbeitsplätze direkt oder indirekt von der Gesundheitsbranche abhängig sind (mehr als im Maschinenbau und in der Autoindustrie zusammen). Auch hat – im Gegensatz zu anderen Branchen – die Zahl der Beschäftigten im Gesundheitswesen in den letzten fünf Jahren um fast 10 % zugenommen. Es gibt rd. 39 000 Ärzte im Land, davon rd. 16 000 in eigener Praxis. Daneben fast 8 000 Zahnärzte und rd. 6 300 Apotheker/-innen in den rd. 2 800 öffentlichen Apotheken.

Dass der gesamte Sozial- und Gesundheitsbereich in dem Bemühen, einen weiteren Anstieg der Kosten zu verhindern und dabei das bestehende Angebot möglichst beizubehalten oder noch zu verbessern, mehr denn je umkämpft ist, bekamen viele Bürger nicht zuletzt auch durch streikende Ärzte an öffentlichen Kliniken und geschlossenen Praxen vor Ort hautnah zu spüren. Ebenso durch von den Versicherten als bürokratisch empfundene intensivere Prüfungen, Rückfragen und Recherchen ihrer Krankenkassen, insbesondere wenn es um Abrechnungen oder die Beantragung bestimmter Leistungen ging. Auch soll nach Aussagen der Deutschen Krankenhausgesellschaft die Zahl von Einzelfallprüfungen durch den Medizinischen Dienst der Krankenversicherungen dadurch drastisch zugenommen haben, dass die Krankenkassen deutlich mehr Krankenhausrechnungen anzweifeln. Dies führt im Ergebnis ebenfalls zu mehr bürokratischem Aufwand, der gerade als erklärtes (Teil-)Ziel der Gesundheitsreform reduziert werden soll.

Hohe Kosten und deren Ursache standen auch im Mittelpunkt der Diskussion um ein anderes Reformvorhaben, das der Öffentlichkeit unter dem Schlagwort „Hartz IV“ bekannt ist. Bei der zu Beginn des Jahres 2005 in Kraft getretenen Arbeitsmarktreform kehrt keine Ruhe ein: Zum 1. August dieses Jahres trat eine umfangreiche Gesetzesänderung in Kraft. Der Entwurf des sog. Gesetzes zur Fortentwicklung der Grundsicherung für Arbeitsuchende war erst im Mai 2006 in den Bundestag eingebracht worden. Dass hier leider wenig Zeit blieb, um sich über den im Grundgesetz verankerten Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen Gedanken zu machen, liegt auf der Hand. Weitere Gesetzesänderungen im Bereich der Grundsicherung für Arbeitsuchende sind im Gespräch.

Dass das Gesundheits- und Sozialwesen und die Überlegungen zum Umbau der sozialen Sicherungssysteme in der bisherigen Form aus den oben genannten Gründen immer mehr zu einem Hauptthema in der Innenpolitik wurden,

bekam unser Amt in diesem Jahr durch eine wiederum gestiegene Anzahl von Anfragen und auch Eingaben sehr deutlich zu spüren. Dies bereitet zunehmend Probleme, da die Personalausstattung der Dienststelle seit Jahren stagniert und die Komplexität und Schwierigkeit der Vorgänge – allein wenn man die rasante Entwicklung im EDV-Bereich betrachtet – immer größer wird. Erfreulich dabei ist, dass unser Rat auch von den öffentlichen Stellen mehr denn je gefragt war. Andererseits denkt man leider oft erst auf den „letzten Drücker“ an die Aspekte des Datenschutzes. Auch hier sollte man unserem Amt das Motto, das im Zusammenhang mit der Verschiebung der Gesundheitsreform neuerdings sehr oft bemüht wurde („Gründlichkeit geht vor Schnelligkeit“), in gleicher Weise zugestehen.

Nicht minder anspruchsvoll und intensiv war die Befassung der Dienststelle auch mit verschiedenen universitären Forschungsvorhaben. Hier gilt das oben Gesagte in besonderer Weise, wonach eine gründliche Befassung mit den meist sehr anspruchsvollen und oftmals auch international verzweigten Projekten einen ausreichenden Zeitvorlauf für eine fundierte datenschutzrechtliche Beratung beansprucht. Besonders ärgerlich ist, wenn im Rahmen eines gesetzlich vorgeschriebenen Genehmigungs-/Beteiligungsverfahrens die Universitäten völlig zu Recht zunächst die zuständigen Ministerien ansprechen und diese dann die anfragenden Wissenschaftler – ohne überhaupt eigene Prüfungen anzustellen – nur an uns verweisen. Hier erwarten wir, dass die Ministerien zukünftig zunächst eine eigenverantwortliche summarische Rechtsprüfung und Bewertung auch dahin gehend vornehmen, ob durch das konkrete Forschungsvorhaben Persönlichkeitsrechte der betroffenen Probanden tangiert und verletzt sein könnten. Ebenso wenig hinnehmbar ist, wenn Ministerien Forschungsvorhaben mit der Maßgabe der Zustimmung unserer Dienststelle (als „Auflage“) genehmigen und dabei offenkundig ist, dass es gerade in diesem Bereich noch viele offene Fragen gibt – mithin das Projekt nicht ansatzweise genehmigungsfähig ist. Eine Änderung dieser Verfahrensweise ist dringend geboten.

## 1. Abschnitt: Gesundheit

### 1. Die elektronische Gesundheitskarte

Mit dieser Thematik hatten wir uns bereits in unserem 26. Tätigkeitsbericht für das Jahr 2005 sehr ausführlich befasst (LT-Drucksache 13/4910). Wir möchten daher an dieser Stelle über die in der Zwischenzeit eingetretene weitere Entwicklung des IT-Projekts berichten.

Gingen wir im letzten Jahr noch davon aus, dass die „elektronische Gesundheitskarte“ (eGK) entsprechend der gesetzlichen Zeitvorgabe in § 291 a des Fünften Buchs des Sozialgesetzbuchs (SGB V) spätestens zum 1. Januar 2006 zum Einsatz kommen wird, gilt inzwischen auch bei diesem Reformvorhaben die Parole: Qualität geht vor Schnelligkeit. Aus datenschutzrechtlicher Sicht kann dies durchaus gut und sinnvoll sein, allerdings nur dann, wenn die Zeit dafür genutzt wird, qualitative Fortschritte im Interesse der Patientenrechte zu erzielen. Dass sich dieses Verfahrensmotto am Ende positiv für das lt. Gesundheitsministerin Ulla Schmidt „größte IT-Projekt der Welt“ auswirken wird, ist zu hoffen. Ein gesundes Maß an Skepsis scheint dennoch angebracht zu sein, da die bisher eingetretenen Verzögerungen nach unserer Wahrnehmung zum geringsten Teil auf Bemühungen der Gematik GmbH, die Datenhoheit der Versicherten zu verbessern, zurückzuführen waren.

Bei der Gematik GmbH handelt es sich bekanntlich um eine eigens geschaffene Gesellschaft, der Krankenkassen und Verbände der Leistungserbringer angehören. Sie hat entsprechend ihrem gesetzlichen Auftrag bei der Einführung der elektronischen Gesundheitskarte die Koordinierungs- und Betreiberfunktion in Bezug auf die Telematikinfrastruktur übernommen und muss die dafür in Betracht kommende Lösungsarchitektur prüfen und auch technisch realisieren. Obwohl die verschiedenen Phasen der Testung in einer eigens dafür vom Bundesministerium für Gesundheit erlassenen Rechtsverordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte vom 2. Oktober 2006 (Bundesgesetzblatt I, Nr. 45,

S. 2189 ff.) genauer beschrieben wurden, sehen wir die Gefahr, dass bei wachsendem Zeitdruck die Versuchung größer werden könnte, bisher entstandene Verzögerungen zumindest teilweise dadurch auszugleichen, dass die Testverfahren sowohl zeitlich wie auch inhaltlich verkürzt werden.

Ich sehe es daher als eine wichtige Aufgabe für meine Dienststelle an, bei der Einführung der elektronischen Gesundheitskarte darauf zu achten, dass der in der o. g. Verordnung sehr präzise vorgegebene Migrationsplan zur Einführung dieses IT-Projekts entsprechend den dort näher beschriebenen vier Teststufen unter Wahrung der Belange des Datenschutzes Schritt für Schritt auch umgesetzt wird. Nur wenn es gelingt, bei den betroffenen Versicherten von Anfang an Vertrauen in die Sinnhaftigkeit und die Seriosität dieses Projekts zu schaffen, kann das Vorhaben zum Nutzen aller Beteiligten zu einem erfolgreichen Ende gebracht werden.

Zum aktuellen Sachstand lässt sich für unseren Kontrollbereich Folgendes mitteilen: Wie eingangs bereits erwähnt, ist die in § 291 a SGB V vorgesehene Frist zur Einführung der elektronischen Gesundheitskarte zum 1. Januar 2006 längst verstrichen. So wurden vom Bundesministerium für Gesundheit erst im Januar 2006 acht Testregionen – darunter der Stadt- und der Landkreis Heilbronn – benannt, die zunächst mit jeweils maximal 10 000 Versicherten, 15 bis 25 Ärzten, fünf Apotheken und einem Krankenhaus die Tests unter realen Einsatzbedingungen, das heißt unter Verwendung von Echtdaten der Versicherten und der Leistungserbringer – selbstverständlich nur mit deren ausdrücklichem schriftlichen Einverständnis – durchführen sollen. Nach unseren Informationen dürfte mit einem Testbeginn inzwischen nicht mehr vor dem Frühjahr 2007 zu rechnen sein. Bei erfolgreichem Verlauf soll dieser Zehntausender-Feldtest in einem weiteren Test mit bis zu 100 000 Versicherten und einer entsprechend größeren Zahl von Leistungserbringern fortgesetzt werden. Hierfür ist nach den bisherigen Planungen neben zwei weiteren Testregionen außerhalb Baden-Württembergs auch Heilbronn vorgesehen. Im Februar 2005 wurde eigens dafür die „Arbeitsgemeinschaft zur Einführung der elektronischen Gesundheitskarte in Baden-Württemberg, ARGE eGK“ gegründet, deren Arbeit wir u. a. in dem gebildeten Beirat auch weiterhin beratend begleiten werden. Ziel der ARGE und auch von uns ist es, in der Testregion Heilbronn im Echtbetrieb Erfahrungen zu sammeln, damit die neue Karte und die dazugehörende Telematikinfrastruktur datenschutzkonform und möglichst gut vorbereitet flächendeckend implementiert werden kann. Wir und unsere Kollegen in den anderen Testregionen werden aber ein strenges Auge darauf haben, dass auch während der Testphase der Datenschutz gewahrt wird und niemand der Versuchung unterliegt, den sich abzeichnenden Zeitverzug von insgesamt rd. zwei Jahren auf Kosten der Qualität und insbesondere der Datensicherheit wieder hereinzuholen. Bedauerlich ist, dass zum Zeitpunkt der Drucklegung dieses Berichts die Gematik GmbH noch immer nicht in der Lage war, ihr schon seit längerer Zeit angekündigtes Datenschutzkonzept vorzustellen.

## 2. Datenschutz im Gesundheitsamt – ein Kontrollbesuch

Den in die Landratsämter eingegliederten Gesundheitsämtern sind im Bereich des öffentlichen Gesundheitswesens zahlreiche Aufgaben zugewiesen. Sie reichen von der Seuchenbekämpfung, der Gesundheitsförderung und -prävention, der Durchführung von Einschulungsuntersuchungen, der Gesundheitsberichterstattung und von epidemiologischen Untersuchungen bis hin zur Erteilung von Auskünften aus dem vertraulichen Teil der Todesbescheinigungen.

Da die Bürgerinnen und Bürger von diesen Themen oft unmittelbar betroffen sind, erhalten wir hierzu eine Vielzahl von Eingaben und auch telefonischen Anfragen. Ebenso stehen wir häufig bei Fragen des Ministeriums für Arbeit und Soziales, aber auch bei Direktanfragen von Gesundheitsämtern Rede und Antwort. Nachdem unser letzter Kontrollbesuch bei einem Gesundheitsamt inzwischen doch einige Zeit zurückliegt (21. Tätigkeitsbericht, LT-Drucksache 12/5740), hielten wir es für angezeigt, wieder einmal vor Ort zu prüfen, ob die seinerzeit bei anderen Gesundheitsämtern festgestellten Mängel endgültig der Vergangenheit angehören oder noch immer anzutreffen sind. Sollen unsere Ausführungen in den Tätigkeitsberichten

doch auch für andere Dienststellen eine Orientierungshilfe sein und diese ermuntern, die dort angesprochenen Themen im Zusammenwirken mit ihren behördlichen Datenschutzbeauftragten anzugehen und gleichgelagerte Mängel zu beseitigen.

Unsere Vor-Ort-Kontrolle führte uns dieses Mal in ein Landratsamt im südlichen Baden-Württemberg.

2.1 Postlauf

Bei vielen Aufgaben des Gesundheitsamts bedarf es eines Erstkontakts mit den Probanden, und dies meist in schriftlicher Form. Wer danach selbst in schriftlicher Form seine Rückmeldung an das Gesundheitsamt richtet, darf zu Recht erwarten, dass sein Schreiben dort auch beim zuständigen Mitarbeiter eingeht. Dies ist datenschutzrechtlich insbesondere deshalb von Belang, weil darin nicht selten bereits sensible Gesundheitsdaten mitgeteilt werden. Besondere Probleme treten immer dann auf, wenn sich das Gesundheitsamt nicht im Hauptgebäude des Landratsamts, sondern in einer Außenstelle befindet, wie wir dies bei unserem Kontrollbesuch vor Ort angetroffen haben.

Wie wir feststellen mussten, gab es beim Landratsamt gleichwohl keine schriftliche Dienstanweisung, die geregelt hätte, wie mit der für das Gesundheitsamt bestimmten Post zu verfahren ist. Die in der Poststelle tätigen Personen hatten stattdessen ein „eigenes“ Verfahren entwickelt, das nach Auskunft eines Mitarbeiters der Poststelle „von Person zu Person“ mündlich weitergegeben wurde. Learning by doing spielte dabei anscheinend die wichtigste Rolle. Schreiben, die erkennbar an das Gesundheitsamt oder dort beschäftigte Personen gerichtet sind, werden nach dieser mündlich überlieferten Praxis verschlossen weitergegeben. Nur allgemein an das Landratsamt adressierte Briefe werden hingegen geöffnet und auf sicherem Weg dem für die interne Postverteilung zuständigen Bediensteten des Gesundheitsamts im Rahmen des Postaustauschs zugeleitet. Schriftstücke des Gesundheitsamts nach außerhalb werden in der Außenstelle selbst gefertigt und vor Ort einkuvertiert, so dass Unbefugte von deren Inhalt keine Kenntnis nehmen können. Sie werden danach zur Poststelle des Hauptgebäudes gebracht, dort frankiert und versandt.

Gegen dieses Postlaufverfahren ist aus Sicht des Datenschutzes grundsätzlich nichts einzuwenden. Allerdings sollte eine schriftliche Fixierung des Verfahrens erfolgen, um z. B. bei Urlaubs- und Krankheitsvertretungen bzw. bei einem Mitarbeiterwechsel, der durchaus nicht immer planbar ist, für einen aus datenschutzrechtlicher Sicht weiterhin reibungslosen Weiterbetrieb zu sorgen. Allerdings ist zu bemängeln, dass Schreiben des Gesundheitsamts an die Probanden als Rückadresse lediglich die Postanschrift des Hauptgebäudes des Landratsamts enthalten. Um zu vermeiden, dass Dritte unnötig Kenntnis von unter Umständen sensiblen Gesundheitsdaten der Probanden nehmen können, sollten diese in den Anschreiben ausdrücklich darum gebeten werden, die Rückmeldungen direkt an die Außenstelle des Landratsamts oder noch besser an den zuständen Bearbeiter beim Gesundheitsamt zu senden. Die uns zunächst im Rahmen des Kontrollbesuchs genannte Begründung, dass dies deshalb nicht gehe, weil sich nur beim Hauptgebäude ein Nachtbriefkasten befinde, der zeitgenau den Briefeinwurf dokumentiere, erwies sich bei näherer Betrachtung als wenig stichhaltig. Fakt ist, dass es bei Posteingängen für das Gesundheitsamt in aller Regel nicht auf eine exakt zu dokumentierende Zeit (z. B. zur Wahrung von Rechtsmitteln) ankommt. Wir haben deshalb das Landratsamt gebeten, auch für das Rückmeldeverfahren eine schriftliche Regelung in einer noch zu erstellenden Dienstanweisung aufzunehmen und die Vordruckschreiben des Gesundheitsamts im Sinne der oben gemachten Ausführungen zu überarbeiten. Eine Rückmeldung des Landratsamts hierzu steht bisher noch aus.

2.2 Ärztliche Untersuchung

Das Gesundheitsamt nimmt nach § 12 des Gesundheitsdienstgesetzes (ÖGDG) ärztliche Untersuchungen vor und erstellt hierüber Gutachten,

Zeugnisse oder Bescheinigungen, wenn dies durch entsprechende Rechtsvorschriften (z. B. im Landesbeamtenrecht) so vorgesehen ist. Auftraggeber ist dabei z. B. ein Schul- oder Finanzamt, das einen entsprechend formulierten Untersuchungsauftrag an das Gesundheitsamt richtet.

Vor der eigentlichen ärztlichen Untersuchung steht die Kontaktaufnahme mit dem Probanden. Von diesem lässt sich das Gesundheitsamt schriftlich erklären, dass er den Arzt des Gesundheitsamts für die Übermittlung des Ergebnisses dieser amtsärztlichen Untersuchung gegenüber der anfordernden Behörde von der Schweigepflicht entbindet. Auf dem gleichen Vordruck erklärt der Proband sein Einverständnis, dass der Amtsarzt seinerseits Auskünfte oder Krankengeschichten, die dieser für Zwecke der Untersuchung für notwendig hält, bei anderen Stellen auch einholen darf. Dies ist aus datenschutzrechtlicher Sicht grundsätzlich in Ordnung. Allerdings wäre zu überlegen, ob die beiden Entbindungserklärungen nicht so gestaltet werden können, dass der Proband mit Hilfe eines Ankreuzsystems die Wahlmöglichkeit hat, differenziert darüber zu entscheiden, ob er möglicherweise seine Entbindungserklärung ausschließlich gegenüber der anfordernden Behörde erklären will und nicht – wie dies bisher nur möglich ist – im Ganzen einwilligen kann oder – als andere Alternative – sein Einverständnis im Ganzen versagen muss. Wir haben dem Gesundheitsamt deshalb empfohlen, die Vordrucke im Sinne einer solchen Wahlmöglichkeit zu überarbeiten.

Im Rahmen von amtsärztlichen Untersuchungen bedient sich das Gesundheitsamt des Vordrucks „Angaben zur Vorgeschichte“, der im Internet auf der Homepage des Gesundheitsamts aufgerufen werden konnte. Wie uns beim Kontrollbesuch gesagt wurde, sollte die Anamnese des Amtsarztes dadurch verkürzt werden, dass der Proband Fragen des Vordrucks bereits in Ruhe zu Hause beantwortet. Der Vergleich eines uns anlässlich des Kontrollbesuchs ausgehändigten Vordruckmusters mit der Internet-Version ergab allerdings bereits inhaltliche Abweichungen. So bestand z. B. eine Abweichung darin, dass im Internet zusätzlich zu den Stammdaten und zum Beruf der Probanden noch weitere Angaben, die ausdrücklich als „freiwillig“ gekennzeichnet waren (Telefon, Fax, E-Mail), erfragt wurden. Dadurch könnte ein Proband im Umkehrschluss fälschlicherweise folgern, dass er die Angaben zu seinem Beruf zwingend beantworten muss.

Zusätzlich zu den Stammdaten in diesen Vordrucken ist ein schriftlicher Hinweis an die Probanden enthalten, wonach eine richtige und vollständige Vorgeschichte eine wesentliche Voraussetzung für ein zutreffendes amtsärztliches Zeugnis sei und sie deshalb gebeten würden, die entsprechenden Fragen so richtig und vollständig wie möglich zu beantworten. Ohne dass dies optisch entsprechend hervorgehoben wäre – was aus datenschutzrechtlicher Sicht zu bemängeln ist – kommt erst danach der Hinweis, dass der Proband die Angaben überhaupt nur im Falle einer (gesetzlich) bestehenden Untersuchungsverpflichtung machen muss. Wir meinen, dass dies eine zentrale Information für den Bürger ist, die nicht erst unter „ferner liefen“ auftauchen sollte.

Mein Amt hat daher dem Landratsamt mitgeteilt, dass diese Gestaltung des Vordrucks in Verbindung mit der sich vom sonstigen Text nicht abhebenden Unterschriftszeile am Ende des Vordrucks nicht den datenschutzrechtlichen Anforderungen des § 4 Abs. 3 LDSG, auf den § 14 Satz 3 ÖGDG verweist, entspricht. So stellt § 4 Abs. 3 Satz 2 LDSG eindeutig klar, dass Einwilligungen, die zusammen mit anderen Erklärungen schriftlich erteilt werden, bereits in ihrem äußeren Erscheinungsbild deutlich vom sonstigen Textbild hervorzuheben sind. Eine Rückäußerung der Behörde hierzu steht noch aus.

Zu unseren Fragen nach dem Inhalt des Vordrucks wurde zunächst erklärt, dass alle Angaben vom Amtsarzt auch ohne entsprechenden Vordruck im Rahmen der Anamnese für die Erstellung der unterschiedlichen Gutachten benötigt würden. Wir mussten dem Gesundheitsamt daraufhin mitteilen, dass nicht jede dieser Fragen, deren Beantwortung unter Umständen interessant und vielleicht auch wünschenswert wäre, auch

tatsächlich für den vorgesehenen konkreten Untersuchungszweck (zwingend) „erforderlich“ und „geeignet“ sein dürfte. Dies ist aber nach den Vorgaben des Bundesverfassungsgerichts in seinem sog. Volkszählungsurteil vom 15. Dezember 1983 (Hinweis: nachzulesen auf unserer Homepage im Internet unter *http://www.baden-wuerttemberg.datenschutz.de)* elementare Voraussetzung für einen zulässigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen (bei Pflichtangaben) und muss nach unserer Auffassung auch entsprechend gelten, wenn es sich „nur“ um sog. freiwillige Angaben der Betroffenen handelt. Auch im letzteren Fall bedarf es einer Beschränkung auf das sachlich Notwendige. Eine Vorratsdatensammlung ist per se unzulässig.

Konkret haben wir das Gesundheitsamt auf die im Vordruck für Frauen vorgesehene Frage angesprochen, ob sie eine regelmäßige Periode haben. An anderer Stelle wird im Vordruck gefragt, ob Familienmitglieder eine Nervenkrankheit oder sonstige bedeutsame Erkrankungen aufweisen. Außerdem – um ein weiteres Beispiel zu nennen – wird grundsätzlich nach Alter und den Ursachen des Todes von Familienmitgliedern gefragt. Dass es von vornherein eine nicht unerhebliche Anzahl von Begutachtungsaufträgen geben wird, für die diese Datenerhebung schlicht überflüssig ist, bedarf keiner näheren Erläuterung. Zwar ist einzuräumen, dass es in der Praxis nicht immer einfach sein wird, für alle denkbaren Fälle von amtsärztlichen Untersuchungen passende Vordrucke zur Vorgeschichte zu entwickeln. Gerade deshalb sollte man von fachlicher Seite auch einmal grundsätzlich darüber nachdenken, ob das Verfahren, so wie es bisher praktiziert wurde (Einstellung eines „Universalvordrucks“ ins Internet bzw. Zusendung eines solchen zusammen mit der Schweigepflichtentbindungserklärung), zukünftig überhaupt noch in dieser Weise fortgesetzt werden soll.

Datenschutzrechtlich korrekt und unbedenklich wäre es, wenn – ausgerichtet am jeweiligen konkreten Untersuchungsauftrag – von medizinischer Seite überlegt würde, welche Fragen auch im Rahmen einer schriftlichen Voraberhebung dem Probanden sinnvollerweise zu stellen sind. Überflüssiges und für das Gutachten nicht Erhebliches hat auch in einem Vordruck nichts zu suchen und muss durch Schwärzung oder Streichung für den Probanden als von diesem nicht zu beantworten deutlich gekennzeichnet werden. Wenn dies nicht geht oder der damit verbundene Aufwand zu hoch ist, müsste die bisherige Verfahrensweise umgestellt werden und der Erhebungsbogen – was in der Praxis wohl durchaus auch geschieht – regelmäßig nur noch zusammen mit dem Amtsarzt vor Ort und mit dessen fachlicher Beratung ausgefüllt werden. Das Landratsamt wurde auf diese Mängel und auf die Notwendigkeit ihrer Beseitigung deutlich hingewiesen. Eine Reaktion steht bisher noch aus.

2.3 Einschulungsuntersuchung

Das Gesundheitsamt untersucht nach § 8 des Gesundheitsdienstgesetzes zur Schule angemeldete Kinder sowie Schülerinnen und Schüler. Die Untersuchung hat den Zweck, gesundheitliche Einschränkungen, die die Schulfähigkeit oder die Teilnahme am Unterricht betreffen, festzustellen. Bei solchen Untersuchungen erhebt das Gesundheitsamt naturgemäß besonders sensible und daher in besonderer Weise geschützte personenbezogene Daten der betroffenen Kinder. Vor diesem Hintergrund stellt sich u. a. die bereits wiederholt an uns herangetragene Frage, ob betroffene Kinder und deren Erziehungsberechtigte zur Teilnahme an solchen Untersuchungen und zur darüber hinausgehenden Angabe von Daten, etwa durch das Ausfüllen eines Erhebungsvordrucks oder das Vorlegen von Dokumenten (z. B. des Impfbuchs oder des sog. gelben Hefts über die Früherkennungsuntersuchungen), rechtlich verpflichtet sind. Die – nach unserer Einschätzung – klare Antwort auf diese Frage ergibt sich aus § 91 des Schulgesetzes für Baden-Württemberg (SchG). Danach sind Schüler verpflichtet, sich im Rahmen der Schulgesundheitspflege durch das Gesundheitsamt überwachen und untersuchen zu lassen, wobei die Pflicht zur Untersuchung auch für die zur Schule angemeldeten Kinder besteht. Für Kinder, die noch nicht

eingeschult wurden (die also noch keine Schüler sind), ist daraus zu schließen:

– Diese Kinder sind nur dann verpflichtet, sich vom Gesundheitsamt untersuchen zu lassen, wenn sie bereits zur Schule angemeldet wurden.

– Eine Rechtspflicht dieser Kinder oder der jeweiligen Erziehungsberechtigten, darüber hinaus Angaben zu machen oder Dokumente vorzulegen, besteht nicht.

Nach § 14 Abs. 1 LDSG muss das Gesundheitsamt bei der Erhebung personenbezogener Daten im Rahmen von Einschulungsuntersuchungen die Betroffenen darauf hinweisen, dass Daten aufgrund einer Rechtsvorschrift erhoben werden, die zur Auskunft verpflichtet. Andernfalls muss das Gesundheitsamt die Betroffenen auf die Freiwilligkeit ihrer Angaben hinweisen. Bei Verwendung eines Erhebungsvordrucks ist auch auf das Bestehen von Auskunfts- und Berichtigungsrechten hinzuweisen. Das vom Gesundheitsamt praktizierte Verfahren, wie es uns im Verlauf des Kontrollbesuchs dargestellt wurde, warf mit Blick auf diese Vorschriften einige datenschutzrechtliche Fragen auf und ließ auch Unzulänglichkeiten erkennen:

2.3.1 Zum Einladungsschreiben an die Eltern mit Erhebungsvordruck

Das Gesundheitsamt verwendet gegenüber Eltern, deren Kinder „demnächst ... eingeschult“ werden, einen Vordruck „Einladung zur Einschulungsuntersuchung“, dessen Rückseite zur Eintragung von „Angaben der oder des Sorgeberechtigten“ in einen ebenfalls vorgedruckten Text vorgesehen ist. Das Einladungsschreiben enthält u. a. die Aussage, dass die Teilnahme an der Untersuchung gemäß § 91 SchG Pflicht sei, sowie die Aufforderung, den rückseitig ausgefüllten Bogen, das Impfbuch und das gelbe Heft über die Früherkennungsuntersuchungen „unbedingt“ mitzubringen. Die Fragen auf der Rückseite des Vordrucks beziehen sich u. a. auf die frühkindliche Entwicklung (z. B. „Laufen gelernt bis zum 18. Monat?“, „Störungen der Sprachentwicklung?“, „Tag und Nacht sauber mit ca. 4 Jahren?“) und auf bisherige Krankheiten und „Besonderheiten“.

Dazu ist aus datenschutzrechtlicher Sicht zu sagen: Mit der Aussage, dass die Teilnahme an der Untersuchung gemäß § 91 SchG Pflicht sei, sollen die Betroffenen offenbar auf eine Rechtspflicht hingewiesen werden. Nach dem Wortlaut des Vordrucks ist nicht eindeutig, dass der Vordruck vom Gesundheitsamt nur in solchen Fällen verwendet wird, in denen die betroffenen Kinder bereits zur Schule angemeldet sind. Somit ist der Vordruck geeignet, in den Fällen, in denen ein Kind noch nicht zur Schule angemeldet ist, den falschen Eindruck zu vermitteln, dass nach § 91 SchG auch in diesen Fällen eine Pflicht zur Teilnahme besteht. Der Vordruck müsste deshalb so überarbeitet werden, dass die Adressaten ohne weiteres erkennen können, ob eine Rechtspflicht nach § 91 SchG gegeben ist oder ob eine Teilnahme freigestellt ist. Das Problem könnte auf einfache Weise etwa dadurch ausgeräumt werden, dass im Vordruck des Gesundheitsamts der nach den Einschulungsuntersuchungsrichtlinien des Sozialministeriums vom 17. November 2004 vorgesehene Text „Die Teilnahme an der Einschulungsuntersuchung ist gemäß § 91 des Schulgesetzes für Baden-Württemberg Pflicht, sobald die Anmeldung des Kindes zur Schule erfolgt ist.“ verwendet wird.

Die Aufforderung, den rückseitig ausgefüllten Bogen, das Impfbuch und das gelbe Heft über die Früherkennungsuntersuchungen „unbedingt“ mitzubringen, lässt nicht erkennen, ob die sich aus den genannten Unterlagen ergebenden Angaben freiwillig sind oder ob die Betroffenen zu solchen Angaben rechtlich verpflichtet sind und aus welchen Rechtsvorschriften sich eine solche Verpflichtung ergibt. Auch insofern kommt eine einfache Lösung

unter Rückgriff auf die Einschulungsuntersuchungsrichtlinien in Betracht, indem das Gesundheitsamt den vom Sozialministerium vorgesehenen Text „Die Beantwortung der Fragen und die Vorlage der Dokumente sind freiwillig.“ verwendet.

Hinsichtlich des Erhebungsvordrucks konnten wir nicht feststellen, dass die Betroffenen vom Gesundheitsamt auf das Bestehen von Auskunfts- und Berichtigungsrechten hingewiesen werden. Solche Hinweise sind im Vordruck nicht enthalten. Der Vordruck müsste entsprechend ergänzt werden.

2.3.2 Zum Dokumentationsbogen

Die Ergebnisse der jeweiligen Einschulungsuntersuchungen werden vom Gesundheitsamt in einem Dokumentationsbogen festgehalten. Soweit die nach diesem Dokumentationsbogen vorgesehenen Angaben den Vorgaben der Einschulungsuntersuchungsrichtlinien entsprechen, gehen wir derzeit davon aus, dass diese Angaben zur Aufgabenerfüllung des Gesundheitsamts erforderlich sind und daher mit dem datenschutzrechtlichen Erforderlichkeitsgrundsatz in Einklang stehen. Dazu ist anzumerken, dass mein Amt die Einschulungsuntersuchungsrichtlinien bislang keiner vertieften datenschutzrechtlichen Prüfung unterzogen hat. Soweit der Dokumentationsbogen des Gesundheitsamts zusätzliche Angaben vorsieht, die sich aus den Einschulungsuntersuchungsrichtlinien nicht ergeben (etwa zu „Graphomotorik/Stifthaltung“, „Visuomotorik“, „Einbeinhüpfen: vorwärts auf 1 Bein“), konnten wir nicht erkennen, zu welchem Zweck und auf welcher Rechtsgrundlage diese personenbezogenen Daten vom Gesundheitsamt erhoben und verarbeitet werden. Ich habe das Landratsamt dazu um Stellungnahme gebeten.

Selbstverständlich sollen die aus datenschutzrechtlicher Sicht erfreulichen Feststellungen hier nicht unter den Tisch fallen. Der Umstand, dass der Vordruck des Gesundheitsamts für Angaben der oder des Sorgeberechtigten abweichend von den Vorgaben der Einschulungsuntersuchungsrichtlinien die Fragen „Hört Ihr Kind häufig nicht zu, wenn Sie etwas mit ihm besprechen?“, „Hat Ihr Kind besondere Ernährungsgewohnheiten?“ und „Treibt Ihr Kind Sport in einer Gruppe/einem Verein?“ nicht enthält, ist aus unserer Sicht unter Berücksichtigung des Gebots der Datenvermeidung zu begrüßen. Zudem teilte uns das Gesundheitsamt mit, dass es im Zusammenhang mit Einschulungsuntersuchungen erhobene personenbezogene Daten grundsätzlich bei sich behält und insbesondere nicht an Schulen übermittelt. Das Gesundheitsamt erklärte, dass solche Daten an Schulen nur dann weitergegeben werden, wenn Erziehungsberechtigte einen Antrag auf vorzeitige Aufnahme oder Zurückstellung stellen und sie sich mit einer solchen Weitergabe einverstanden erklären.

2.4 Aktenführung

Ein Abstecher in die Registraturen gehört inzwischen zu einem festen Bestandteil unserer Prüfungen vor Ort. Sie sind für Datenschützer ein ergiebiger Quell der Erkenntnis und oft Spiegelbild dafür, wie ernsthaft die unserer Kontrolle unterliegenden öffentlichen Stellen gewillt sind, die elementaren Grundregeln des Datenschutzes zu beachten. An entsprechenden Hinweisen hat es schon in unseren früheren Tätigkeitsberichten nicht gefehlt. Sie alle aufzuführen, wäre zu umfänglich, so dass wir uns hier auf einen Hinweis in unserem 21. Tätigkeitsbericht des Jahres 2000 mit dem Titel „Das Gesundheitsamt vergisst nichts“ beschränken möchten (vgl. LT-Drucksache 12/5740).

Selbstverständlich kann nichts dagegen eingewandt werden, wenn eine Behörde Akten anlegt und diese auch archiviert. Dies gilt selbstredend auch für die Dokumentation der vom Gesundheitsamt durchgeführten Untersuchungen. Für die Tätigkeit der Amtsärzte kann in Anlehnung an die ärztliche Berufsordnung sogar von einer Dokumentationspflicht

ausgegangen werden. Kritisch wird es allerdings dann, wenn Patienten- bzw. Probandendaten in zu großem Umfang oder zu lange gespeichert werden und dies in einer Art und Weise geschieht, dass dadurch eine datenschutzrechtlich unzulässige Kenntnisnahme durch Unbefugte ermöglicht wird.

Bei einer stichprobenweisen Überprüfung von in der Hängeregistratur aufbewahrten Akten des Gesundheitsamts mussten wir feststellen, dass ohne Rücksicht auf den konkreten Untersuchungsauftrag und deren Abschluss alle Vorgänge in einer Akte über viele Jahre hinweg aufbewahrt wurden. Wie bereits oben dargestellt, sind die Aufgaben eines Gesundheitsamts vielfältig; es gibt – wie wir uns vor Ort überzeugen konnten – nicht selten Fälle, in denen ein und dieselbe Person aus unterschiedlichen Anlässen mit dem Gesundheitsamt in Kontakt kommt. Bei der angetroffenen Art der Aktenführung führt dies im Ergebnis dazu, dass sog. Personalakten über die Patienten/Probanden entstehen. In der behördlichen Praxis hat dies dann zur Folge, dass bei einem neuen, dieselbe Person betreffenden Untersuchungsauftrag die gesamte „Patientenakte“ ohne fachliche Notwendigkeit dem mit dem neuen Untersuchungsauftrag beauftragten Amtsarzt auf dessen Anforderung hin von der Registratur zugeleitet wird.

Diese Verfahrensweise ist weder mit der in § 203 des Strafgesetzbuchs geschützten ärztlichen Schweigepflicht, die bekanntlich auch zwischen den Ärzten gilt, vereinbar noch mit dem datenschutzrechtlichen Erforderlichkeitsgrundsatz, wie er sich aus § 15 ÖGDG bzw. § 14 ÖGDG in Verbindung mit §§ 13 ff. LDSG ergibt. Das Gesundheitsamt muss sich deshalb der Mühe unterziehen, zukünftig die Aktenablage so zu gestalten, dass abgeschlossene Untersuchungsaufträge aktenmäßig tatsächlich auch so behandelt werden. Nach einer Registrierordnung, die dies verbindlich festschreibt, haben wir beim Gesundheitsamt vergeblich gesucht. Wir haben daher in unserem Kontrollbericht an das Landratsamt sehr deutlich auf den entsprechenden Nachholbedarf hingewiesen.

Ergänzend angemerkt sei in diesem Zusammenhang noch, dass wir bei unserer Kontrolle auch feststellen mussten, dass in den Hängeordnern der Registratur Akten über verschiedene Personen mit gleichem Anfangsbuchstaben gemeinsam abgelegt waren. Aus datenschutzrechtlicher Sicht vorzugswürdig wäre, wenn jeder Proband einen eigenen Ordner hätte. Dadurch würde von vornherein vermieden, dass Unterlagen mit sensiblem Inhalt von anderen Personen mit gleichem Anfangsbuchstaben versehentlich in den Bearbeitungsgang beim Gesundheitsamt gelangen.

Das Recht des Einzelnen auf Datenschutz wird immer dann verletzt, wenn eine öffentliche Stelle zeitlich unbegrenzt und ohne sachliche Notwendigkeit Informationen über seine Person speichert. Eine Speicherung ist grundsätzlich nur so lange zulässig, wie diese Daten zur Aufgabenerfüllung auch tatsächlich benötigt werden (§ 23 LDSG). Wenn eine Typisierung von Löschfristen in der Behördenpraxis nicht möglich ist, richten sich diese nach den konkreten Umständen des Einzelfalls. Für das Gesundheitsamt und dort tätige Amtsärzte kann allerdings in Anlehnung an die ärztliche Berufsordnung von einer regelmäßigen Aufbewahrungsdauer von zehn Jahren nach Abschluss der Untersuchung ausgegangen werden. Diese Frist wurde nach unseren Feststellungen vor Ort beachtet, was hier ausdrücklich lobend erwähnt werden soll. Ebenso, dass kürzere, durch besondere Rechtsvorschriften vorgegebene Aufbewahrungsfristen (z. B. Infektionsschutzgesetz) ebenfalls beachtet wurden. Vermisst haben wir leider eine schriftliche Dienstanweisung dazu. Damit diese richtige Verwaltungspraxis auch weiterhin und von einem Personalwechsel oder einer Vertretungssituationen unabhängig funktioniert, haben wir empfohlen, dies in einer noch zu erstellenden Registraturordnung für das Gesundheitsamt ebenfalls mit aufzunehmen.

Aufbewahrungsfristen und Aktenvernichtung sind zwei wichtige Aspekte, die datenschutzrechtlich eng miteinander verwoben sind. Auch hier ist einiges beim Datenschutz zu beachten, worauf wir schon wiederholt in früheren Tätigkeitsberichten hingewiesen haben. Bei dem

kontrollierten Gesundheitsamt wird das zur Vernichtung anstehende Schriftgut in verschließbaren Containern, die eine darauf spezialisierte Firma dort aufstellt, gesammelt, danach abgeholt und schließlich auch geschreddert. Dies ist an und für sich ein geeignetes und datenschutzkonformes Vorgehen. Zu bemängeln war dabei nur, dass eine entsprechende Verfahrensbeschreibung bislang noch keinen Eingang in eine schriftliche Dienstanweisung für die Mitarbeiter gefunden hatte. Es kann daher für diese unklar sein, welche Schriftstücke wegen ihres Personenbezugs bzw. Inhalts einer speziellen Behandlung bedürfen und bei welchen es ausreicht, wenn sie lediglich über einen Papierkorb im Büro entsorgt werden. Auf diese Mängel haben wir das Landratsamt ebenso aufmerksam gemacht wie darauf, dass auch noch geregelt werden müsste, ob und wer ausnahmsweise Akten des Gesundheitsamts mit entsprechend sensitivem Inhalt mit nach Hause nehmen darf. Um dienstliche Vorgänge außerhalb des Amts bearbeiten zu können, müssen besondere technische und organisatorische Vorkehrungen zur Gewährleistung des Datenschutzes im häuslichen Umfeld beachtet werden. Wegen der konkreten Ausgestaltung sollte hier der fachkundige Rat des behördlichen Datenschutzbeauftragten des Landratsamts eingeholt werden. Auf § 10 LDSG wird ausdrücklich hingewiesen.

2.5 Das EDV-Verfahren „Octoware“

Das von einem privaten Unternehmen entwickelte EDV-Verfahren Octoware wird, wie wir bereits anlässlich früherer Kontrollbesuche bei Gesundheitsämtern feststellen mussten, von diesen häufig als Softwareprogramm verwendet. Davon konnten sich meine Mitarbeiter auch bei ihrem jüngsten Kontrollbesuch überzeugen. Mit ihm sollen insbesondere die im Zusammenhang mit der Durchführung amtsärztlicher Untersuchungen bzw. mit der Erfassung meldepflichtiger Krankheiten anfallenden Daten EDV-unterstützt verarbeitet werden. Auch wird das Programm beispielsweise eingesetzt, wenn das Gesundheitsamt Aufgaben im Rahmen des Bestattungsrechts wahrnimmt.

Dass ein EDV-Verfahren dienende Funktion hat und gerade dazu entwickelt wird, die Abläufe technisch zu unterstützen, ist an und für sich eine Binsenweisheit. Ebenso, dass sich das EDV-Verfahren am geltenden Recht auszurichten hat und nicht umgekehrt. Leider mussten wir vor Ort feststellen, dass Octoware diesen Anforderungen jedenfalls in Teilbereichen nicht gerecht wird, obwohl wir anlässlich früherer Kontrollbesuche schon gravierende Mängel feststellen mussten, die von uns seinerzeit auch beanstandet wurden.

So erfasst Octoware im Gegensatz zur manuellen und papierenen Aktenbetreuung in seiner Software in einer Zentralkartei alle Personen, die jemals mit dem Gesundheitsamt Kontakt hatten, nicht nur lebenslang, sondern sogar über den Tod hinaus. Dies liegt daran, dass dieses Programm keine Lösch- und Aussonderungsregelungen enthält. Bei unserer Kontrolle haben wir beispielsweise festgestellt, dass vom Gesundheitsamt aufgrund des Bestattungsrechts Abrechnungsdaten von Todesbescheinigungen gespeichert wurden, deren administrative Bearbeitung schon längst abgeschlossen war. Vor Ort konnten uns auch keine plausiblen Gründe genannt werden, für welche sonstigen amtsärztlichen Zwecke diese Angaben noch weiterhin benötigt werden. Wir mussten dem Landratsamt in unserem Kontrollbericht daraufhin mitteilen, dass fehlende bzw. mangelhafte EDV-technische Unterstützung durch Software nicht davon entbindet, gegebenenfalls entsprechende eigene Lösch- und Aussonderungsregelungen/-maßnahmen zu treffen oder alternativ diese Maßnahmen sogar manuell vorzunehmen.

Die Nutzung von Octoware erfordert eine Benutzeranmeldung mit Benutzerkennung und Passwort. Zu den vom System gewährleisteten Passwortkonventionen ist Folgendes anzumerken:

– Das System stellt technisch keine Passwort-Mindestlänge sicher,

– es gibt keinen automatischen Verfall der Passwörter nach einer gewissen Zeit,

– es gibt keine Sperre nach mehreren Anmeldeversuchen und

– es gibt keine Passworthistorie, die verhindert, dass bei einem Passwortwechsel eines der letzten Passwörter wieder verwendet wird.

Der von Octoware gewährleistete Passwortschutz entspricht somit nicht den datenschutzrechtlichen Anforderungen, wie sie z. B. in unseren Hinweisen zum Umgang mit Passwörtern dokumentiert sind. Wir haben daher das Landratsamt gebeten, die Passwortkonventionen entsprechend anzupassen und – sofern das Programm keine entsprechenden Konventionen ermöglicht – beim Hersteller des Verfahrens auf eine entsprechende Anpassung hinzuwirken. Dies gilt im Übrigen, worauf das Landratsamt rein vorsorglich hingewiesen wurde, nicht nur bei Octoware, sondern auch bei der Nutzung anderer EDV-Verfahren, mit denen das Landratsamt personenbezogene Daten verarbeitet. Eine Rückmeldung von Seiten des Landratsamts steht bisher noch aus.

## 3. Einzelfälle

### 3.1 Zettelwirtschaft bei der Essensausgabe im Krankenhaus

Dass betroffene Personen bei Daten über ihre Gesundheit meist sehr empfindlich reagieren, ist keine Überraschung. Insbesondere dann nicht, wenn es sich wie vorliegend um ein Zentrum für Psychiatrie handelt. Auch zunächst wenig spektakulär klingende Hinweise zum Umgang mit personenbezogenen Daten im Krankenhausalltag sind dabei durchaus ernst zu nehmen.

Von einem früheren Patienten eines Zentrums für Psychiatrie wurden wir darüber informiert, dass dort die Ausgabe des Mittag- bzw. Abendessens über ein Tablettsystem abgewickelt werde. Damit das Wunschessen den richtigen Besteller erreiche, würden zuvor die Tabletts mit Namenszetteln gekennzeichnet. Beim Abräumen der Tabletts blieben diese Namenszettel nach seiner Beobachtung oft auf den Tabletts liegen und würden zum Teil im Rücklauf in die Küche bzw. im Altpapier der jeweiligen Station landen. Selbst bei seinen Spaziergängen im Klinikgelände habe er Zettel mit Patientennamen gefunden, die ebenfalls von der Essensausgabe stammten.

In der von uns daraufhin vom Zentrum für Psychiatrie erbetenen Stellungnahme wurde berichtet, dass die Patienten im Vorfeld der Essensbestellung einen Speiseplan erhielten und sich aus dem Angebot das gewünschte Essen auswählen könnten. Die Essensbestellungen würden danach von den Stationen nach den Vorgaben der Patienten EDV-unterstützt an die Klinikküche weitergemeldet. Dabei würden der Küche neben Angaben über die Patientennamen auch deren Stationszugehörigkeit sowie der jeweilige Essenswunsch übermittelt. In der Küche selbst würden diese Angaben dann vom Küchenleiter bzw. seinem Stellvertreter auf Namenszetteln ausgedruckt, damit dort bereits eine stations- bzw. namensbezogene Tablettierung der Essen durchgeführt werden könne. Die Auslieferung der Tabletts selbst erfolge in geschlossenen Essenswagen. Nach den im Krankenhaus getroffenen Verfahrensregelungen müssten die Namenszettel nach dem Essen durch das Stationspersonal wieder mit abgeräumt und in eigens dafür vorgehaltene Datenschutzbehälter entsorgt werden. Ein Rücklauf dieser Zettel in die Küche dürfte daher – wenn immer vorschriftsmäßig verfahren würde – nicht stattfinden. So weit die Theorie. In der Praxis – so jedenfalls unser Eindruck – nahm man diese Anweisung nach dem Motto „Papier ist geduldig“ nicht ganz so ernst. Unserem Amt gegenüber musste man daher im Wesentlichen auch die von dem Petenten beschriebenen Nachlässigkeiten im Umgang mit den Namenszetteln einräumen.

Dass an Krankenzimmern angebrachte Namenszettel von Patienten ohne ihre ausdrückliche vorherige Einwilligung deren Persönlichkeitsrechte verletzen, dürfte inzwischen (hoffentlich) datenschutzrechtliches Allgemeingut im Krankenhausalltag sein. Ebenso wenig kann es daher angehen, dass Besucher oder auch Mitpatienten „über den Umweg“ der

Essensausgabe im Krankenhausflur oder gar bei einem Spaziergang im Freigelände erfahren, wer (Mit-)Patient im Zentrum für Psychiatrie ist.

Von einer förmlichen Beanstandung dieses Datenschutzverstoßes habe ich abgesehen, weil das Krankenhaus für diesen Bereich schon interne Regelungen getroffen hatte und sich bei der Aufarbeitung der Eingabe sehr kooperativ und einsichtig zeigte. So nahm man die Eingabe zum Anlass, die zuständigen Abteilungsleiter erneut auf den korrekten Umgang mit den Namenszetteln der Patienten beim Rücklauf der Essentabletts zu erinnern. Als weitere Maßnahme wurde in der Küche selbst eine Datenschutzbox aufgestellt, um für eine datenschutzkonforme Entsorgung der Namenszettel für die Fälle zu sorgen, in denen diese dennoch versehentlich einmal zusammen mit den Tabletts in die Küche gelangen sollten. Darüber hinaus erging von Seiten der Klinikleitung die Anweisung an den behördlichen Datenschutzbeauftragten, die praktische Umsetzung im Klinikalltag zu überwachen. Für uns blieb allerdings die Frage im Raum, weshalb solche Nachlässigkeiten erst durch die Einschaltung unseres Amts aufgedeckt werden mussten. Es sollte doch zu den ureigensten Aufgaben eines Datenschutzbeauftragten in einem Krankenhaus gehören, sich vor Ort mit wachem Auge zu vergewissern, dass leicht erkennbare Unzulänglichkeiten im Umgang mit Patientendaten – trotz allem Verständnis für die oftmals nicht einfache personelle Situation in den Krankenhäusern – von vornherein nicht vorkommen. Sollten sie dennoch einmal geschehen, hat der Datenschutzbeauftragte die notwendigen Maßnahmen für eine rasche Behebung zu veranlassen.

### 3.2 Ausweiskopien für die Ausstellung der elektronischen Gesundheitskarte

Es dürfte sich inzwischen bei den Krankenversicherten herumgesprochen haben, dass die Einführung der elektronischen Gesundheitskarte mit der umfassenden Ausgabe von neuen Chipkarten einhergeht, die die bisherige Versichertenkarte ersetzen sollen. Dazu wird eine neue, lebenslang gültige Krankenversichertennummer vergeben, die die frühere Versichertennummer ersetzen soll. Zwischen den Spitzenverbänden der Krankenkassen und der Deutschen Rentenversicherung wurde hierfür auf Bundesebene ein Datenabgleich zwischen den Krankenkassen und der Rentenversicherung für Personen vereinbart, die bereits im Besitz einer Krankenversichertennummer sind. Begründet wurde dieses Vorgehen damit, dass sowohl für die Rentenversicherung als auch für die Krankenversicherung die Korrektheit der Schreibweise von Vor- und Familienname zwingende Voraussetzung für eine eindeutige Zuordnung des einzelnen Versicherten sei.

Rechtsgrundlage für diese Handlungsweise ist der im Rahmen des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung neu geschaffene § 290 des Fünften Buchs des Sozialgesetzbuchs. Verbunden mit der Einführung der elektronischen Gesundheitskarte ist die Abkehr der Krankenkassen von ihrem bisherigen System, bei dem jede Kasse eine eigene Bearbeitungsnummer für jeden ihrer Versicherten vergeben hatte. Bei häufigen Kassenwechseln und damit ständig wechselnden Nummern wären mit dem alten System insbesondere die mit dem Gesetz verfolgten Ziele, wie z. B. die Vornahme von arzt- bzw. versichertenbezogenen Zufälligkeitsprüfungen bei der Medikation, nicht zu erreichen gewesen. So weit, so gut.

Nicht unsere Billigung fand allerdings das Verhalten einer gesetzlichen Krankenkasse, die sich zur Vorbereitung der Ausgabe der neuen Krankenversichertenkarte in einem Serienbrief an ihre Mitglieder wandte. Von der nachstehend näher beschriebenen Vorgehensweise der Kasse erfuhren wir aber erst durch mehrere Eingaben: In dem Serienbrief wurden die Versicherten zunächst (kurz) darüber informiert, dass moderne elektronische Gesundheitskarten die bisherigen Krankenversichertenkarten ersetzen sollen und sie dafür eine neue Krankenversichertennummer benötigten. Deshalb – so die Versicherung weiter – brauche jeder Versicherte eine gültige Rentenversicherungsnummer mit aktuellen Daten. Danach wurden die Versicherten nur noch darüber informiert, dass sie bereits im Besitz ihrer ganz persönlichen Rentenversicherungs-

nummer seien. Erst am Ende kam die Krankenkasse dann zu ihrem eigentlichen Anliegen, indem sie die Versicherten bat, ihr zwecks Überprüfung der Richtigkeit der hinterlegten Daten eine Personalausweiskopie zu senden. Kundennah erklärte sich die Krankenversicherung in diesem Schreiben abschließend noch bereit, die Portokosten für die Versicherten zu übernehmen bzw. ihnen die Möglichkeit zu geben, diese Kopien kostenlos in ihren Kundencentern zu fertigen.

Auf die datenschutzrechtliche Bedenklichkeit dieses Vorgehens von uns angesprochen, schrieb uns die Krankenkasse, dass sowohl für die Rentenversicherung als auch für die Krankenversicherung die Korrektheit der Schreibweise von Vor- und Familienname für eine eindeutige Zuordnung des einzelnen Versicherten zwingende Voraussetzung sei. So habe der aus diesem Grund mit dem Datenbestand der Deutschen Rentenversicherung durchgeführte Datenabgleich allein bei ihren Mitgliedern in rd. 50 000 Fällen Abweichungen bei der Namensschreibweise ergeben. Um eine eindeutige Zuordnung der betroffenen Personen sicherzustellen und um abzuklären, wie die korrekte Schreibweise von Vor- und Familienname der betroffenen Versicherten sei, habe man sich dazu entschieden, dies direkt mit den betreffenden Versicherten abzuklären. Zu diesem Zweck habe man den Mustertext mit dem oben wiedergegebenen Inhalt und der Bitte um Übersendung einer Personalausweiskopie entworfen. Dieses Verfahren sei in einem Testlauf erprobt worden, wobei keine der angeschriebenen Personen datenschutzrechtliche Bedenken gegenüber der Krankenkasse geäußert hätte. Auch handele es sich um eine einmalige Aktion im Rahmen der Umsetzung des Projekts „Neue Krankenversichertennummer“, so dass die Kopien der Personalausweise unverzüglich nach der vollständigen Klärung des Sachverhalts datenschutzkonform vernichtet würden. Schließlich teilte man uns noch mit, dass man unabhängig von der Einführung der neuen elektronischen Gesundheitskarte auch zukünftig nicht umhin komme, durch eine persönliche Kontaktaufnahme mit den Versicherten die korrekte Schreibweise zu ermitteln und zu dokumentieren.

Der Krankenkasse haben wir daraufhin mitgeteilt, dass ihre Vorgehensweise insbesondere deshalb nicht den Regeln des Datenschutzes entspreche, weil die angeforderten Kopien der Personalausweise auch einige Angaben enthalten, die von der Krankenkasse nicht für die Prüfung der korrekten Schreibweise der Namen ihrer Versicherten benötigt werden. So enthalten Personalausweisdokumente Angaben über die Größe, die Farbe der Augen, unveränderliche Kennzeichen, das Lichtbild und die Personalausweisnummer des Inhabers. Nach § 67 a des Zehnten Buchs des Sozialgesetzbuchs bzw. § 13 Abs. 1 LDSG ist das Erheben personenbezogener Daten nur insoweit zulässig, als ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle auch tatsächlich erforderlich ist. Korrekt wäre es daher gewesen, wenn die Krankenkasse ihre Versicherten ausdrücklich darauf hingewiesen hätte, zu welchem konkreten Zweck sie die Ausweiskopie benötigt und dass es den Versicherten anheim gegeben wird, die nicht benötigten Angaben auf der Ausweiskopie durch Schwärzungen unkenntlich zu machen. Ohne Belang ist hierbei der Hinweis an die Versicherten, wonach diese die Ausweise in den Kundencentern unentgeltlich kopieren können. Sicherlich wird die Qualität einer guten Versicherteninformation nicht automatisch mit zunehmender Länge besser; in der Kürze soll ja sprichwörtlich die Würze liegen. Dies gilt allerdings nur dann, wenn diese – im Gegensatz zu der vorliegenden Kundeninformation – nicht so knapp gerät, dass am Ende für die Betroffenen mehr Fragen als Antworten übrig bleiben. Es greift der allgemeine datenschutzrechtliche Grundsatz, nach dem die Betroffenen angemessen über den mit der Datenverarbeitung verfolgten Zweck aufzuklären sind (§ 4 Abs. 2 LDSG).

Nachdem die Krankenkasse rasch reagiert und meiner Dienststelle zugesagt hat, künftig in den Anschreiben detaillierter auf die Gründe für die Notwendigkeit der Vorlage von Ausweiskopien durch die Versicherten sowie darauf hinzuweisen, dass dafür nicht benötigte Angaben geschwärzt werden können, habe ich von einer förmlichen Beanstandung abgesehen.

## 2. Abschnitt: Die gesetzliche Krankenversicherung

### 1. Anforderung von Einkommensteuerbescheiden

Bei der beitragsrechtlichen Einstufung ihrer freiwillig versicherten Mitglieder gibt es immer wieder Fälle, in denen gesetzliche Krankenkassen ihre Versicherten zur Vorlage von aktuellen Einkommensteuerbescheiden auffordern bzw. entsprechende Anfragen direkt an die Finanzämter richten. Uns erreichten Anfragen besorgter Bürger, ob ein solches Vorgehen durch die einschlägigen datenschutzrechtlichen Bestimmungen gedeckt sei. Unsere Antwort darauf lautete wie folgt:

Nach § 240 Abs. 1 Satz 2 des Fünften Buchs des Sozialgesetzbuchs (SGB V) in Verbindung mit den einschlägigen Krankenkassensatzungen erfolgt die Beitragsberechnung für freiwillig versicherte Mitglieder anhand ihrer wirtschaftlichen Leistungsfähigkeit, die konkret und individuell durch die Krankenkasse zu überprüfen ist. Berechnungsgrundlage ist dabei die gesamte wirtschaftliche Leistungsfähigkeit des freiwilligen Mitglieds. Eine Prüfung der Verhältnisse im Einzelfall hinsichtlich der tatsächlich erzielten (Gesamt-)Einnahmen ist daher grundsätzlich erforderlich und der Krankenkasse demzufolge auch gestattet (§ 284 Abs. 1 Nr. 3 SGB V in Verbindung mit § 67 a Abs. 1 des Zehnten Buchs des Sozialgesetzbuchs – SGB X). Nach dem im Datenschutzrecht geltenden Direkterhebungsgrundsatz müssen diese Daten von den Krankenkassen jedoch regelmäßig bei den Betroffenen selbst erhoben werden. Ohne deren Mitwirkung dürfen sie nur ausnahmsweise und in den wenigen in § 67 a Abs. 2 SGB X genannten Fällen bei Dritten – wozu an sich auch Finanzämter zählen – erhoben werden. Im Zusammenhang mit der Anforderung von Einkommensteuerbescheiden durch die gesetzlichen Krankenkassen dürften allerdings die in dieser Vorschrift genannten Ausnahmefälle regelmäßig nicht greifen, so dass an dieser Stelle auch nicht näher darauf eingegangen werden soll.

Nach dem in § 20 Abs. 1 SGB X normierten Untersuchungsgrundsatz ist die Krankenkasse verpflichtet, Sachverhaltsermittlungen von Amts wegen durchzuführen. Sie bestimmt dabei Art und Umfang der Ermittlungen, wobei sie an das Vorbringen und an die Beweisanträge der Beteiligten nicht gebunden ist. Es liegt vielmehr in ihrem pflichtgemäßen Ermessen, welcher Beweismittel sie sich dafür bedient. Auf die sich aus dem Direkterhebungsgrundsatz ergebenden Einschränkungen (§ 67 a Abs. 2 SGB X) weisen wir in diesem Zusammenhang nochmals ausdrücklich hin.

Den Nachweis der wirtschaftlichen Leistungsfähigkeit hat der Versicherte gemäß § 206 SGB V durch die Vorlage von Unterlagen gegenüber der Krankenkasse zu erbringen. Er ist der Krankenkasse gegenüber auch verpflichtet, auf Verlangen Auskunft über alle für die Feststellung der Versicherungs- und Beitragspflicht und für die Erledigung der ihr übertragenen Aufgaben erforderlichen Tatsachen zu erteilen. Ebenso hat der Versicherte auf Verlangen der Krankenkasse Unterlagen, aus denen sich Tatsachen oder Änderungen für das Versicherungsverhältnis ergeben, vorzulegen. Die Aufforderung zur Vorlage eines Einkommensteuerbescheids – verbunden mit dem Hinweis, dass die für die Beitragsberechnung nicht benötigten Daten vom Versicherten geschwärzt werden können – ist demzufolge durch die genannten Bestimmungen des Sozialgesetzbuchs gedeckt und kann somit auch datenschutzrechtlich nicht beanstandet werden. Nach unserer Beobachtung entspricht dieses Verfahren grundsätzlich auch der gängigen Krankenversicherungspraxis; unstatthafte Direktanfragen bei den Finanzämtern bilden dabei glücklicherweise die unrühmliche Ausnahme.

### 2. Kundenwerbung im Pfarrbüro

Mehr Wettbewerb unter den Krankenkassen war ein erklärtes Ziel des im Jahr 2003 beschlossenen Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung. Als weder mit diesem Gesetz noch mit dem Landesdatenschutzgesetz vereinbar und offensichtlich von einigen Marketingstrategen in deren Kundencentern gründlich missverstanden erwies sich allerdings eine Mitgliederwerbeaktion bei Arbeitgebern, über die wir von einem Pfarrbüro (als Arbeitgeber) informiert wurden. Was war geschehen? Dem uns übermittelten Vordruckschreiben konnten wir entnehmen, dass die

Krankenkasse die Kirchengemeinde als Arbeitgeber angeschrieben und darum gebeten hatte, die bei ihr beschäftigten Auszubildenden namentlich und unter Angabe weiterer personenbezogener Daten zu nennen. Damit aber nicht genug. Die Krankenkasse wollte in den dem Serienbrief beigefügten Erhebungsbogen darüber hinaus auch noch nähere Informationen über Vorname, Name und Telefonnummer der Ausbildungsleiter erhalten.

Auf schriftliche Nachfrage räumte die Krankenkasse unumwunden ein, dass die Datenerhebung durch das Kundencenter ohne die vorherige Einwilligung der Betroffenen und deshalb in unzulässiger Weise erfolgt sei. Ein entsprechender Hinweis auf dem Anschreiben sei versehentlich unterblieben. Auf unsere Bitte hin, zusätzlich in Erfahrung zu bringen, ob entsprechende Anschreiben auch anderweitig Verwendung gefunden hätten, teilte man mit, dass solche Anfragen nur ausnahmsweise und in Fällen vorgekommen seien, in denen z. B. eine telefonische Kontaktaufnahme mit den Arbeitgebern trotz mehrfacher Bemühungen nicht möglich gewesen sei. Man informierte uns ferner darüber, dass diese Art der Kundenwerbung nur bei wenigen Bezirksdirektionen in ähnlicher Weise vorgekommen sei, ohne dass es für die Krankenkasse im Nachhinein möglich wäre, solche Aktionen zahlenmäßig genauer zu beziffern.

Aus datenschutzrechtlicher Sicht fiel uns die Bewertung nicht sonderlich schwer, da die Rechtslage eindeutig ist: Gemäß § 4 Abs. 1 LDSG ist eine Verarbeitung personenbezogener Daten, wozu auch die Datenerhebung zählt, nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene in die Erhebung eingewilligt hat. Beide Voraussetzungen waren im vorliegenden Fall nicht gegeben.

Bei der Krankenkasse hat man auf unsere Hinweise sehr professionell und rasch reagiert und im Rahmen einer Arbeitstagung mit verantwortlichen Mitarbeitern aus den Bereichen „Kunden und Vertrieb“ diesen Fall datenschutzrechtlich problematisiert. Ihnen wurde exemplarisch aufgezeigt, welche rechtlichen Anforderungen an eine datenschutzkonforme Datenerhebung im Rahmen einer Kundenwerbung zu richten seien. Man hat uns auch zugesichert, die bemängelten Anschreiben an die Arbeitgeber mit sofortiger Wirkung nicht mehr zu verwenden. Zur weiteren Schadensbegrenzung habe man die Mitarbeiter der Krankenkasse angewiesen, in Fällen, in denen Arbeitgeber bereits entsprechende Angaben gemacht hätten, mit den Betroffenen nachträglich noch persönlich Kontakt aufzunehmen. Für den Fall, dass diese sich danach mit der Speicherung und Nutzung ihrer Daten nicht ausdrücklich einverstanden erklären sollten, seien die Mitarbeiter angehalten worden, die seinerzeit unzulässig erhobenen Daten unverzüglich zu löschen. Diese Anweisung entspricht der Bestimmung des § 23 LDSG.

Das Bemühen um umfassende Sachverhaltsaufklärung sowie um Schadensbegrenzung durch die oben näher beschriebenen Maßnahmen haben mich im Rahmen der Abwägung der Gesamtumstände dazu veranlasst, von einer förmlichen Beanstandung gegenüber der Krankenkasse abzusehen. Ich gehe davon aus, dass die getroffenen Maßnahmen derzeit ausreichend sind und auch in Zukunft greifen müssten, damit entsprechende Datenschutzverstöße im Rahmen von Werbeaktionen zur Gewinnung von Neukunden nicht mehr auftreten.

## 3. Abschnitt: Soziales

### 1. Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende

Bereits beim Erscheinen unseres Tätigkeitsberichts für 2005 waren die Kostenexplosion bei „Hartz IV“ und ihre Ursachen Thema in Politik und Medien. Die Debatte um die Kosten hält an. Die Gründe, die für die unerwarteten Kostensteigerungen genannt werden, sind vielfältig: So sollen z. B. Statistiken, auf deren Grundlage Experten Anfang 2003 berechnet haben, wie viele Menschen Anspruch auf die Grundsicherung für Arbeitsuchende haben, bereits zum damaligen Zeitpunkt überholt gewesen sein. Weiter sei eine große Anzahl der Menschen, die heute Arbeitslosengeld II beziehen, gar nicht arbeitslos, verdiene aber in ihrem Job so wenig, dass sie Zulagen erhielten; bei den Planungen der Grundsicherung für Arbeitsuchende sei

diese Personengruppe nicht ausreichend berücksichtigt worden. Als Faktor für den Kostenanstieg werden auch psychologische Aspekte genannt: Viele Bezieher von Arbeitslosengeld II hätten auch früher Anspruch auf Sozialhilfe gehabt, diese aber nicht beantragt, da sie den Gang zum Sozialamt scheuten. Vorgetragen wird außerdem, dass die sog. Hartz-Gesetze Barrieren zum Bezug staatlicher Hilfe gesenkt hätten.

Mancher Politiker hat die hohen Kosten der Grundsicherung für Arbeitsuchende mit Missbrauch in großem Stile zu erklären versucht. Fragwürdiger Natur waren die Quellen, auf deren Basis solche Behauptungen aufgestellt wurden: Die Telefonbefragung der Bundesagentur für Arbeit im Sommer 2005 war jedenfalls keine geeignete Methode zur Erfassung von Missbrauch. Dass Leistungsempfänger wiederholt nicht ans Telefon gingen oder die telefonische Befragung, die ausdrücklich freiwillig erfolgen sollte, ablehnten, lässt keine entsprechenden Rückschlüsse zu.

Gleichwohl wurde im Mai dieses Jahres von den Fraktionen der CDU/CSU und der SPD der Entwurf eines Gesetzes zur Fortentwicklung der Grundsicherung für Arbeitsuchende (BT-Drucksache 16/1410) in den Bundestag eingebracht, der insbesondere auch die Vermeidung von Leistungsmissbrauch zum Ziel hat. Anfang Juni 2006 wurde das Gesetz vom Bundestag beschlossen und trat nach Zustimmung des Bundesrats in seinen überwiegenden Teilen zum 1. August dieses Jahres in Kraft. Die neuen Regelungen zur Vermeidung von Leistungsmissbrauch tangieren den Datenschutz zum Teil erheblich:

– Bei der Frage des Vorliegens einer eheähnlichen Gemeinschaft wurde eine Beweislastumkehr zulasten der Arbeitsuchenden eingeführt: Betroffene müssen seit August dieses Jahres nachweisen, dass sie mit Mitbewohnern, mit denen sie länger als ein Jahr zusammenleben, keine Verantwortungs- und Einstehensgemeinschaft bilden. Die Regelung birgt die Gefahr der Erhebung und Speicherung sensibler Daten in großem Umfang. Auf einem Zusatzblatt zu den Antragsformularen der Bundesagentur für Arbeit werden die Betroffenen inzwischen aufgefordert, möglichst umfassend darzulegen, warum die gesetzliche Vermutung in ihrem Fall nicht greift, und dies durch entsprechende Unterlagen nachzuweisen.

– Die Arbeitsgemeinschaften sollen einen Außendienst zur Bekämpfung von Leistungsmissbrauch einrichten. Die neue Regelung ändert zwar an den rechtlichen Voraussetzungen der Zulässigkeit von Hausbesuchen (z. B. Betretensrecht nur mit vorheriger Zustimmung des Betroffenen) nichts, stellt aber einen Appell an die Leistungsträger dar, Maßnahmen zu ergreifen, die sich im sensiblen Bereich von Artikel 13 des Grundgesetzes (Unverletzlichkeit der Wohnung) bewegen.

– Das Fortentwicklungsgesetz erweitert die Möglichkeiten eines automatisierten Datenabgleichs. Präventive Datenabgleiche sind aber aus verfassungsrechtlichen Gründen wegen des hiermit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung nur dann zuzulassen, wenn sie im vorrangigen öffentlichen Interesse tatsächlich notwendig und verhältnismäßig sind. Als vorrangiges öffentliches Interesse kommen beispielsweise beträchtliche Schäden, die durch unberechtigten Bezug von Leistungen für die Allgemeinheit entstehen, in Betracht. Entsprechende Fakten, die dies belegen können, wurden im Gesetzgebungsverfahren nicht dargelegt.

– Das Gesetz sieht neue Auskunftsmöglichkeiten, z. B. beim Kraftfahrt-Bundesamt, vor. Auch hierdurch wird das informationelle Selbstbestimmungsrecht im Allgemeininteresse stark eingeschränkt. Trotzdem stellt die neue Regelung nicht klar, dass Abfragen nur anlassbezogen, das heißt erst, wenn aufgrund der Angaben der Betroffenen tatsächliche Anhaltspunkte für deren Unrichtigkeit oder Unvollständigkeit bestehen, zulässig sind.

– Schlussendlich wurde die Erhebung, Verarbeitung und Nutzung von Sozialdaten durch nichtöffentliche Stellen dergestalt erweitert, dass zur Erfüllung der Aufgaben nach dem Zweiten Buch des Sozialgesetzbuchs einschließlich der Erbringung von Leistungen zur Eingliederung in Arbeit und Bekämpfung von Leistungsmissbrauch Dritte beauftragt werden

können. Bedenken bestehen, ob die hoheitliche Aufgabe der Befragung von Leistungsempfängern zur Vermeidung von Leistungsmissbrauch auf diese Weise auf nichtöffentliche Stellen übertragen werden kann.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hatte im Gesetzgebungsverfahren gegenüber dem Ausschuss für Arbeit und Soziales des Bundestags zum Gesetzentwurf Stellung genommen und zum Teil erheblichen Nachbesserungsbedarf gesehen. Diesen Appell unterstützten Datenschutzbeauftragte der Länder in einer gemeinsamen Erklärung, in der sie Bundestag und Bundesrat aufforderten, den Gesetzentwurf mit Blick auf das Recht auf informationelle Selbstbestimmung grundlegend zu überarbeiten. Die Bitte, die Anliegen der Datenschutzbeauftragten zu unterstützen, richtete ich auch an das hiesige Ministerium für Arbeit und Soziales. Die Interventionen blieben bisher leider ohne Erfolg.

**2. Weitere Entwicklungen beim Arbeitslosengeld II**

Die umfangreichen Antragsvordrucke der Bundesagentur für Arbeit hatten wir schon in unseren Tätigkeitsberichten für 2004 und 2005 angesprochen. Da nicht alle Fragen in den Vordrucken aus Sicht des Datenschutzes zulässig waren, hatte die Bundesagentur auf Wunsch und mit Unterstützung der Datenschutzbeauftragten Ausfüllhinweise entwickelt und zugesagt, Änderungen am Vordruck bei dessen Neuauflage zu berücksichtigen. Im Laufe des Jahres 2005 überarbeitete die Bundesagentur das Antragsformular und die Zusatzblätter.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte im Oktober 2005 in einer Entschließung, allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den überarbeiteten Ausfüllhinweisen zur Verfügung zu stellen. Der Weg, bis die Antragsteller die neuen Antragsunterlagen tatsächlich in den Händen halten konnten, war jedoch noch weit: Erst seit Juli dieses Jahres sind die überarbeiteten Antragsformulare nebst Ausfüllhinweisen im Internet abrufbar. Nur kurze Zeit später wurde das Zusatzblatt „Vorliegen einer Verantwortungs- und Einstehensgemeinschaft“ ins Internet eingestellt, an deren Erstellung die Datenschutzbeauftragten nicht beteiligt waren. Das Zusatzblatt ist aus Sicht des Datenschutzes bedenklich: Auf dem Formular werden die Antragsteller aufgefordert, möglichst umfassend darzulegen, warum die gesetzliche Vermutung des Vorliegens einer Verantwortungs- und Einstehensgemeinschaft in ihrem Fall nicht greift und dies durch entsprechende Unterlagen nachzuweisen. Wie bereits oben dargestellt (s. Nr. 1), besteht hier die Gefahr einer übermäßigen Preisgabe gerade sensibler Daten. Die Antragsvordrucke werden von der Bundesagentur derzeit insgesamt erneut überarbeitet. Hieran sind auch die Datenschutzbeauftragten beteiligt.

Ebenfalls in unseren Tätigkeitsberichten für 2004 und 2005 berichteten wir von dem Datenbanksystem A2LL, welches die Erfassung und Verwaltung von finanziellen Leistungen für die Bezieher von Arbeitslosengeld II ermöglicht. Hier gibt es jetzt einen Silberstreif am Horizont: Bei der Software A2LL sei inzwischen, wie uns mitgeteilt wurde, eine Protokollierung der Zugriffe programmiert. Ferner hat nach uns vorliegenden Informationen die Bundesagentur für Arbeit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der für die zentralen EDV-Programme zuständig ist, ein Zugriffsberechtigungskonzept vorgelegt. Dieses sehe jedoch weiterhin die Möglichkeit eines bundesweiten Zugriffs auf Daten der Hilfesuchenden vor. Gerade dieser Punkt war aber von den Datenschutzbeauftragten bisher kritisiert worden. Dass das Kapitel A2LL aus Sicht des Datenschutzes bald geschlossen werden kann, ist daher eher unwahrscheinlich.

Das IT-Verfahren VAM/VerBIS (Virtueller Arbeitsmarkt/Vermittlungs-, Beratungs- und Informationssystem) ist inzwischen flächendeckend in den Arbeitsgemeinschaften für die Arbeitsvermittlung in Betrieb genommen worden. Ein Zugriffsberechtigungskonzept liegt vor. Bezüglich des Umfangs der Berechtigungen sieht der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit noch Gesprächsbedarf. Auch bei VAM/VerBIS fehlt bisher ein Protokollierungskonzept. Außerdem erfolgt eine Protokollierung derzeit nur bei schreibendem Zugriff, das heißt wenn Änderungen vorgenommen werden. Eine Protokollierung bei nur lesendem Zugriff gibt

es lediglich bei ärztlichen Gutachten. Der Bundesbeauftragte ist auch in diesem Punkt mit der Bundesagentur im Gespräch.

### 3. Arbeitslosengeld II: Kontrollbesuch bei einer Optionskommune

Wie bereits im Tätigkeitsbericht für 2005 dargestellt, ist gesetzlich vorgesehen, dass die Träger der Leistungen der Grundsicherung für Arbeitsuchende – das sind die Bundesagentur für Arbeit und die kommunalen Träger, d. h. die Stadt- und Landkreise – zur einheitlichen Aufgabenerfüllung jeweils eine Arbeitsgemeinschaft (ARGE) bilden. Fünf Landkreise in Baden-Württemberg haben von der im Gesetz ebenfalls vorgesehenen Möglichkeit Gebrauch gemacht, die Aufgaben in alleiniger Verantwortung zu erfüllen. Eine dieser sog. Optionskommunen war dieses Jahr Ziel eines Kontrollbesuchs unserer Dienststelle: Wir wollten mit eigenen Augen sehen, wie ein kommunaler Träger die Arbeitsmarktreform umgesetzt hat.

#### 3.1 Die Annahmestelle

Bei der Abgabe des Antrags auf Arbeitslosengeld II können so sensible Themen wie eine bestehende Schwangerschaft, Krankheiten, Einkommens- und Vermögensverhältnisse und vieles mehr zur Sprache kommen. Die Beratung der Antragsteller der Grundsicherung für Arbeitsuchende ist daher auch in den Ämtern so zu organisieren, dass Außenstehende keine Kenntnis von den personenbezogenen Daten der Ausfüllenden erlangen können. Dieser Schutz von Sozialdaten war insbesondere kurz nach Einführung des Arbeitslosengelds II nicht überall gewährleistet: Im Tätigkeitsbericht für 2005 berichteten wir bereits von einer ARGE, bei der der organisatorische Zusammenschluss auch räumliche Veränderungen mit sich gebracht hatte und eine den Erfordernissen des Datenschutzes entsprechende Antragsannahme anfangs nicht sichergestellt war.

Auch bei der von uns besuchten Optionskommune war die Vertraulichkeit des gesprochenen Worts nicht in ausreichendem Maße gewährleistet: Die Antragsannahme erfolgte zwar in einem von den Wartenden getrennten Raum, was vorbildlich ist. Der Abstand zwischen den beiden Antragstellern, die bei der Annahme des Antrags gleichzeitig beraten werden, war jedoch nicht ausreichend groß, um die Möglichkeit auszuschließen, dass ein Antragsteller das Gespräch eines anderen Antragstellers mithört. Von den Mitarbeitern der Annahmestelle wurde uns zwar geschildert, dass, falls sich ein Antragsteller über mangelnde Vertraulichkeit beschwere, die beiden Antragsteller einzeln nacheinander beraten werden. Diese Vorgehensweise der Mitarbeiter vor Ort ist aus Sicht des Datenschutzes jedoch nicht ausreichend:

Durch organisatorische Maßnahmen ist generell sicherzustellen, dass die betroffenen Personen von der Möglichkeit einer vertraulichen Beratung zuverlässig Kenntnis erhalten. Zum Beispiel kann im Wartezimmer auf einem gut sichtbaren Schild darauf hingewiesen werden, dass der Betroffene sich auf Wunsch auch einzeln beraten lassen kann. Eine Beratung sollte selbstverständlich und nicht nur ausnahmsweise vertraulich sein. Ein Mithören durch andere Antragsteller muss grundsätzlich ausgeschlossen sein.

Wir haben die Optionskommune gebeten, diese Zielsetzung zu verfolgen, auch wenn sie Umzugs- oder Umbaumaßnahmen der Annahmestelle erfordern kann. Eine Reaktion des Landratsamts hierzu steht noch aus.

#### 3.2 Das Antragsformular

Den langen Weg bis zur Änderung der Antragsformulare der Bundesagentur für Arbeit haben wir bereits geschildert (s. gleicher Abschnitt, Nr. 2). Wir hoffen, dass eine Änderung des Antragsvordrucks für das Arbeitslosengeld II, den die von uns besuchte Optionskommune verwendet, schneller erfolgt. Änderungsbedarf besteht in folgenden Punkten:

– In dem Vordruck für den Antrag auf Leistungen der Grundsicherung für Arbeitsuchende sollen unter anderem Personen aufgeführt werden, die außer dem Antragsteller und dessen Partner mit diesem in

einem Haushalt leben. Über diese Personen werden u. a. Angaben zum höchsten Schulabschluss, zum höchsten Berufsbildungsabschluss, zur derzeit ausgeübten Tätigkeit, zur Krankenkasse, zur Unterbringung in einer stationären Einrichtung und zu Einkommen und Vermögen verlangt. Hierzu ist anzumerken, dass zwischen einer Haushaltsgemeinschaft und einer Bedarfsgemeinschaft zu unterscheiden ist. Wer zur Bedarfsgemeinschaft gehört, ist im Vordruck zu erläutern, um zu verhindern, dass die Antragsteller überschießende Angaben machen, deren Kenntnis für die Aufgabenerfüllung der Optionskommune nicht erforderlich sind.

– Soweit Hilfebedürftige in Haushaltsgemeinschaft mit Verwandten und Verschwägerten leben, besteht die gesetzliche Vermutung, dass sie von diesen Leistungen erhalten, soweit dies nach deren Einkommen und Vermögen erwartet werden kann. Der Antragsteller muss daher in der Regel angeben, ob er Leistungen von diesen Personen erhält. Die Erforderlichkeit von Angaben über diesen Personenkreis zum höchsten Schulabschluss, zum höchsten Berufsausbildungsabschluss, zur derzeit ausgeübten Tätigkeit, zur Krankenkasse und zur Unterbringung in einer stationären Einrichtung leuchtet jedoch nicht ein.

– Am Ende des Antragsvordrucks für das Arbeitslosengeld II erhält die Wohnsitzgemeinde Gelegenheit zur Stellungnahme. Dabei soll die Gemeinde beurteilen, ob die in dem Antrag gemachten Angaben der Wahrheit entsprechen. Das ist nicht zulässig. Zwar werden Anträge auf Sozialleistungen von allen Gemeinden entgegengenommen. Anträge, die bei einer für die Sozialleistung nicht zuständigen Gemeinde gestellt werden, sind aber unverzüglich an den zuständigen Sozialleistungsträger weiterzuleiten. Die Wohnortgemeinde ist dabei nicht gehindert, den Bürger auf seinen Wunsch hin bei der Antragstellung zu beraten, z. B. ihm nicht sofort verständliche Datenfelder zu erläutern oder ihn auf offensichtliche Unvollständigkeiten hinzuweisen. Eine wie auch immer geartete Prüfzuständigkeit, ob die Angaben im Antrag der Wahrheit entsprechen, haben Wohnortgemeinden jedoch nicht. Wir haben die Optionskommune daher aufgefordert, die genannte Rubrik zu streichen.

3.3 Scannen von Antragsunterlagen

Wie wir vor Ort feststellen mussten, wurden bei der von uns besuchten Optionskommune Unterlagen, die von den Antragstellern vorgelegt werden, grundsätzlich eingescannt und zur elektronischen Akte genommen.

Das generelle Kopieren und dauerhafte Speichern der von den Antragstellern vorgelegten Unterlagen, soweit diese personenbezogene Daten enthalten, halten wir nicht für zulässig. Der Leistungsträger hat nach Prüfung der vorgelegten Unterlagen zunächst zu überlegen, ob es nicht ausreichend ist, in der Akte zu vermerken, dass ein bestimmter Nachweis erbracht wurde und, soweit das Datum selbst nicht schon in dem Antrag auf Arbeitslosengeld II etc. angegeben wurde, dieses Datum in der Akte zu vermerken. Soweit ein solcher Vermerk nicht ausreichend sein sollte und die eingereichten Unterlagen eingescannt werden, sind in den eingescannten Unterlagen die Angaben, die nicht leistungsrelevant sind, zu schwärzen.

In diesem Zusammenhang ist aber auch darauf hinzuweisen, dass der Leistungsträger berechtigt ist, die oben angesprochene Prüfung der vorgelegten Unterlagen außerhalb der Sprechzeiten vorzunehmen. Insofern wäre das Verlangen eines Leistungsträgers, die Originalunterlagen oder Kopien von diesen für ein paar Tage zur Einsichtnahme zu behalten, nicht zu beanstanden.

3.4 Wer hat Zugriff auf die elektronische Akte?

Nicht erst wenn Sozialdaten den internen Bereich einer Behörde verlassen, spielt der Datenschutz eine Rolle. Vielmehr ist auch die innerbehördliche Organisation so zu gestalten, dass sie den besonderen An-

forderungen des Datenschutzes gerecht wird. Zum Zeitpunkt unseres Kontrollbesuchs hatten alle ca. 25 Mitarbeiter Zugriff auf die von der Optionskommune elektronisch geführten Akten aller ungefähr 2 500 Bedarfsgemeinschaften. Außerdem wurden ein Leistungsprogramm, mit dem Leistungen nach dem Zweiten Sozialgesetzbuch errechnet und Bescheide erstellt werden, und ein Vermittlungsprogramm genutzt. Auch hier gab es keine Unterscheidungen in den Zugriffsberechtigungen.

Wenn eine Behörde ihren Mitarbeitern eine Zugriffsmöglichkeit für elektronisch gespeicherte Daten einräumt, gibt sie ihnen eine sehr leistungsfähige Möglichkeit an die Hand, in Sekundenschnelle Daten aus einem sehr großen Bestand herauszusuchen und zu bearbeiten. Sofern es sich hierbei um personenbezogene Daten handelt, muss die Behörde dafür sorgen, dass derartige Zugriffsmöglichkeiten nur in dem Umfang erteilt werden, wie sie dienstlich geboten sind. Vorliegend konnten wir eine Erforderlichkeit für die Möglichkeit jedes einzelnen Mitarbeiters, auf alle Bedarfsgemeinschaften zuzugreifen, insbesondere im Bereich des Vermittlungsprogramms, nicht erkennen.

Wir haben die Optionskommune daher gebeten, alle von ihr in diesem Bereich erteilten Zugriffsberechtigungen auf ihre Erforderlichkeit hin zu überprüfen und so zu gestalten, dass jeder Mitarbeiter künftig nur noch auf personenbezogene Daten zugreifen kann, für deren Bearbeitung er zuständig ist oder die er sonst zwingend für die Erfüllung seiner Aufgaben benötigt.

3.5 Die Untersuchung durch das Gesundheitsamt

Arbeitslosengeld II erhält nur, wer erwerbsfähig ist (nicht erwerbsfähige Angehörige, die mit erwerbsfähigen Hilfebedürftigen in Bedarfsgemeinschaft leben, können aber Sozialgeld erhalten). Als erwerbsfähig gilt nach dem Zweiten Buch des Sozialgesetzbuchs, wer nicht wegen Krankheit oder Behinderung auf absehbare Zeit außer Stande ist, unter den üblichen Bedingungen des allgemeinen Arbeitsmarkts mindestens drei Stunden täglich erwerbstätig zu sein. Wir stellten fest, dass die Optionskommune das Gesundheitsamt um eine Untersuchung des Hilfebedürftigen bat, da sie an dessen Erwerbsunfähigkeit zweifelte. Diese Untersuchung kündigte der zuständige Fallmanager dem Hilfebedürftigen zwar an, eine Einwilligung für die ärztliche Untersuchungsmaßnahme holte er von diesem aber nicht ein. Der Fallmanager gab die Daten des Hilfebedürftigen an das Gesundheitsamt weiter. Dieses lud den Hilfebedürftigen anschließend zu einer Untersuchung.

Dieses Vorgehen ist nicht in Ordnung. Die Übermittlung personenbezogener Daten des Hilfebedürftigen an das Gesundheitsamt ist unzulässig, solange die zu untersuchende Person nicht ihre Bereitschaft erklärt hat, sich einer solchen Untersuchung zu unterziehen. Denn den Hilfesuchenden und -empfängern muss es selbst überlassen bleiben, ob sie sich, aus welchen Gründen auch immer, der Untersuchung stellen wollen oder nicht. Allerdings müssen sie dann die sich aus einer Verweigerung möglicherweise ergebenden Konsequenzen (Versagung oder Entziehung von Leistungen aufgrund fehlender Mitwirkung) tragen.

## 4. Was darf der Beistand?

Leben Eltern getrennt, hat der Elternteil, bei dem das Kind nicht lebt, Unterhalt in bar zu leisten. Auf Antrag des anderen Elternteils wird das Jugendamt Beistand des Kindes für die Geltendmachung dieses Unterhaltsanspruchs. Das Jugendamt überträgt die Ausübung der Aufgaben des Beistands einzelnen seiner Beamten oder Angestellten. Dieser wird Vertreter des Kindes, z. B. für die außergerichtliche Verfolgung von Unterhaltsansprüchen im Verhandlungswege und notfalls deren gerichtliche Durchsetzung.

Datenschutzrechtlich ist der Beistand eine gewisse Besonderheit, weil für den Schutz von Sozialdaten bei ihrer Erhebung und Verwendung im Rahmen der Tätigkeit des Jugendamts als Beistand nur eine einzige gesetzliche Regelung gilt, und zwar § 68 des Achten Buchs des Sozialgesetzbuchs

(SGB VIII). Dass es bei Anwendung auch nur einer Vorschrift zu Auslegungsfragen kommen kann, hat ein Fall aus dem Berichtszeitraum gezeigt:

Ein Vater zweier Kinder, die im Rahmen einer Beistandschaft von einem Mitarbeiter des Jugendamts vertreten wurden, wandte sich an unsere Dienststelle. Der Mitarbeiter, der die Beistandschaft ausübte, hatte Klage auf Leistung von Unterhalt gegen den Petenten erhoben. In einem Schriftsatz an das Gericht hatte der Mitarbeiter vorgetragen, der Vater sei womöglich gar nicht mehr arbeitslos; die für ihn zuständige Agentur für Arbeit habe auf Anfrage mitgeteilt, dass der Petent von dort derzeit keine Leistungen beziehe. Hierüber ärgerte sich der verklagte Vater aus zwei Gründen: Erstens sei – wie er uns mitteilte – die Auskunft der Agentur für Arbeit sachlich nicht richtig. Zweitens war der Petent aber auch erstaunt darüber, dass sich das Jugendamt direkt an die Agentur für Arbeit gewandt hatte, obwohl er selbst in der Vergangenheit auf Anfrage stets die gewünschten Auskünfte erteilt und Nachweise vorgelegt habe.

Das von uns um Stellungnahme gebetene Jugendamt berief sich darauf, dass im Rahmen der Tätigkeit des Jugendamts als Beistand – was korrekt ist – nur § 68 SGB VIII gilt. Nach dieser Vorschrift darf der Beamte oder Angestellte, der die Beistandschaft ausübt, Sozialdaten nur erheben und verwenden, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Die Erforderlichkeit der Datenerhebung konnte dem Beistand im vorliegenden Fall nicht abgesprochen werden. Unserer Auffassung nach hätte sich der Mitarbeiter des Jugendamts aber zunächst an den Petenten selbst wenden müssen. Denn auch wenn der Vorrang der Betroffenenerhebung sich nicht aus dem Wortlaut der Regelung des § 68 SGB VIII ergibt, ist dieser unmittelbar aus dem Volkszählungsurteil abzuleiten und ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung: Die Direkterhebung beim Betroffenen dient der Transparenz der Datenerhebung und verhindert, dass Datenverarbeitungen „hinter dem Rücken“ des Betroffenen stattfinden. Das Jugendamt selbst hatte in einem Schreiben an den Petenten ausgeführt, dass dieser auf Anfrage jeweils die gewünschten Auskünfte einschließlich Nachweisen erteilt hatte. Die Datenerhebung des Beistands bei der Agentur für Arbeit hielten wir daher nicht für zulässig.

# 4. Teil: Kommunales und anderes

## 1. Abschnitt: Kommunales

### 1. Unterrichtung der Medien über die Wohnverhältnisse eines Gemeinderatsmitglieds

Ein Mitglied des Gemeinderats einer Großen Kreisstadt erblickte in folgender Vorgehensweise des Oberbürgermeisters einen Datenschutzverstoß: Im Rahmen einer Pressekonferenz habe der Oberbürgermeister Pläne seines Wohn- und Geschäftshauses mittels eines Tageslichtprojektors präsentiert. Diese seien von anwesenden Fernsehjournalisten auch „abgefilmt“ und im Fernsehen gezeigt worden. Ziel dieser Präsentation sei es gewesen darzustellen, dass ihm in diesem Gebäude lediglich zwei kleine Appartements zum Wohnen zur Verfügung stünden. Dieser Eingriff in seine Rechte sei auch nicht durch die aktuelle melde- und kommunalrechtliche Auseinandersetzung zwischen dem Oberbürgermeister und ihm (es ging um die Frage, ob der Stadtrat seine Wohnung bzw. Hauptwohnung in der Großen Kreisstadt hat und ob er die Wählbarkeit noch besitzt) nicht gerechtfertigt gewesen.

Die von uns zur Stellungnahme aufgeforderte Große Kreisstadt teilte uns mit, der Fall sei seit Wochen in der Presse diskutiert worden. Es gehe um die Frage, wo sich die Hauptwohnung des Petenten befinde. Auch durch widersprüchliche Aussagen des Petenten über die von ihm und seiner Familie in dem Gebäude genutzte Wohnung habe sich die Stadt veranlasst gesehen, im Rahmen einer Pressekonferenz „eine umfassende Objektivierung“ vorzunehmen. Dabei sei u. a. der Grundriss einer bestimmten in diesem Wohn- und Geschäftshaus gelegenen Wohnung gezeigt worden, um zu verdeutlichen, dass dort eine dreiköpfige Familie nicht wohnen könne. Während der Pressekonferenz sei dem Oberbürgermeister und seinem Pressesprecher entgangen, dass der Kameramann eines privaten Fernsehsenders offensichtlich Teile der Ausführungen des Oberbürgermeisters gefilmt habe. Eigentlich sei lediglich die Aufnahme eines Kurzstatements des Oberbürgermeisters im Anschluss an die Pressekonferenz vorgesehen gewesen. In rechtlicher Hinsicht berief sich die Stadt insbesondere auf das Informationsrecht der Presse. Ein schutzwürdiges Interesse des Petenten an der Verweigerung der Auskunft lag nach Meinung der Stadt nicht vor.

Wir haben den Sachverhalt datenschutzrechtlich wie folgt beurteilt: Zwar haben die Medien aufgrund der verfassungsrechtlich verankerten Pressefreiheit gegenüber den Behörden einen weitreichenden Informationsanspruch. Allerdings muss, wenn es wie hier um personenbezogene Daten geht, eine Abwägung mit den schutzwürdigen Interessen des Betroffenen stattfinden. Das hat die Große Kreisstadt nicht hinreichend beachtet. Nach dem Meldegesetz sind nämlich Wohnungsgröße und -grundriss weder für die Frage, ob jemand überhaupt eine bestimmte Wohnung bewohnt, noch für den Wohnungsstatus (Haupt- oder Nebenwohnung) relevant. Die Präsentation des Wohnungsgrundrisses gegenüber den Medien war demnach von vornherein nicht geeignet, zur Klärung der Frage, ob der Petent in der Großen Kreisstadt wohnt und dort seine Hauptwohnung hat, beizutragen. Die Stadt hätte deshalb bei der gebotenen Abwägung zum Ergebnis kommen müssen, dass die schutzwürdigen Interessen des Petenten einer Auskunftserteilung an die Medien in dieser Art und Weise entgegenstehen.

Erfreuliches gibt es zu diesem Fall auch noch zu berichten: Der Oberbürgermeister hat zugesagt, die datenschutzrechtlichen Vorschriften künftig zu beachten. Außerdem will er dem Gemeinderat die Bestellung eines behördlichen Datenschutzbeauftragten empfehlen.

### 2. Wie der Störer einer Gemeinderatssitzung an den Pranger gestellt wurde

Ein Bürger und langjähriges Gemeinderatsmitglied einer kleinen Gemeinde wandte sich wegen folgenden Sachverhalts an unsere Dienststelle: Der Bürgermeister habe im Rahmen der Fragestunde des Gemeinderats die Ausführungen eines Fragestellers als beleidigend empfunden und den Betroffenen deshalb aus dem Sitzungssaal verwiesen. Diesen Vorfall habe die Ge-

meinde sowohl in ihrem Mitteilungsblatt als auch auf ihrer Homepage veröffentlicht, und zwar unter namentlicher Nennung des Einwohners. Das Gemeinderatsmitglied sah den Betroffenen dadurch an den Pranger gestellt.

Der von uns angehörte Bürgermeister zeigte sich höchst verwundert über unser „Einschreiten“. Unter anderem verwies er darauf, dass es sich um eine öffentliche Gemeinderatssitzung gehandelt habe und es einer jahre- oder gar jahrzehntelangen Übung der Gemeinde entspreche, ausführlich, d. h. wohl auch personenbezogen, über den Inhalt und Ablauf solcher Sitzungen zu berichten. Der Bürgermeister verstieg sich zu der Behauptung, Einwohner, die sich in der Fragestunde zu Wort meldeten, hätten nichts dagegen, wenn ihr Name in gemeindlichen Veröffentlichungen genannt werde, ja sie legten sogar Wert darauf. In einer späteren Gemeinderatssitzung habe der Betroffene auf seine Frage, inwieweit er Veröffentlichungen im Amtsblatt und im Internet zustimme, erklärt, das könne der Bürgermeister halten wie er wolle.

Wir haben den Sachverhalt datenschutzrechtlich wie folgt beurteilt: Nach § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Eine etwaige Einwilligung hätte vor der Veröffentlichung ausdrücklich erklärt werden müssen. Das war hier nicht der Fall. Auch die Tatsache, dass ein Einwohner sich in öffentlicher Sitzung im Rahmen der Fragestunde zu Wort meldet, berechtigt die Gemeinde nicht dazu, solche Wortmeldungen bzw. bestimmte Umstände in diesem Zusammenhang beliebig weiter zu verbreiten. Die sog. begrenzte Sitzungsöffentlichkeit ist insoweit vergleichbar mit einer öffentlichen Gerichtsverhandlung. Auch Gerichtsurteile dürfen in aller Regel nicht personenbezogen veröffentlicht werden. § 20 Abs. 1 der Gemeindeordnung sieht zwar vor, dass der Gemeinderat die Einwohner durch den Bürgermeister über die allgemein bedeutsamen Angelegenheiten der Gemeinde unterrichtet. Abgesehen davon, dass es sich im vorliegenden Fall wohl kaum um eine solche Angelegenheit gehandelt hat, ist bei personenbezogenen Veröffentlichungen § 18 LDSG zu beachten. Nach dessen Absatz 1 ist die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach § 15 Abs. 1 bis 4 LDSG zulässig wäre, oder der Dritte, an den die Daten übermittelt werden sollen, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Diese Voraussetzungen, die unabhängig davon gelten, ob die Gemeinde personenbezogene Daten im amtlichen oder im nichtamtlichen Teil ihres Mitteilungsblatts veröffentlicht, lagen nicht vor. Weder war die personenbezogene Veröffentlichung zur Aufgabenerfüllung der Gemeinde erforderlich noch durfte die Gemeinde davon ausgehen, dass der Betroffene kein schutzwürdiges Interesse am Ausschluss der Datenübermittlung hat. Die weltweite Verbreitung über das Internet ohne Einwilligung des Betroffenen schied bereits wegen des örtlich begrenzten Aufgaben- und Wirkungskreises der Gemeinden aus.

Wir haben der Gemeinde unsere Rechtsauffassung mitgeteilt und verlangt, dass die Gemeinde den einschlägigen Beitrag unverzüglich von ihrer Homepage entfernt und die datenschutzrechtlichen Vorschriften künftig beachtet.

### 3. Der widerspenstige Staatsdiener

Ein Grundstückseigentümer wandte sich erbost an unsere Dienststelle. Einer Tageszeitung hatte er entnommen, dass der Vertreter einer Kleinstadt dienstlich gewonnene Erkenntnisse, die den Grundstückseigentümer betrafen, im Rahmen einer Radwegeinweihung preisgegeben hatte. Nach dem Pressebericht habe der städtische Vertreter erklärt, bis auf eine Ausnahme habe die Stadt mit den Grundstückseigentümern erfolgreich verhandelt. Dass ausgerechnet ein Staatsdiener mit abstrusen, irrealen und überzogenen Forderungen verhindert habe, dass auch die letzten 50 Meter des Radwegs zum Rest passen (gemeint waren die unterschiedliche Breite sowie Schotter- anstatt Asphaltbelag), ärgere ihn gewaltig. Vielleicht solle man sich nicht scheuen, für die Nutzer des Radwegs an dieser Stelle ein entsprechen-

des Hinweisschild aufzustellen. Schließlich bezeichnete der städtische Bedienstete den Petenten als uneinsichtig. Kein Wunder, dass sich der Petent durch die in Anwesenheit eines Pressevertreters gefallenen Äußerungen öffentlich brüskiert fühlte.

Die von uns zur Stellungnahme aufgeforderte Stadt stellte die oben wiedergegebenen Äußerungen nicht in Abrede. Allerdings sei jegliche Personifizierung unterblieben, so dass keine personenbezogenen Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermittelt worden seien. Gleichzeitig räumte die Stadt aber ein, beim Befahren des Radwegs sei aufgrund der Unterbrechung des ausgebauten Zustands offensichtlich erkennbar, um welches Grundstück es sich handle. Es könne deshalb durchaus nachvollziehbar sein, wer der Eigentümer sei.

Wir haben den Sachverhalt datenschutzrechtlich wie folgt bewertet: Nach dem Landesdatenschutzgesetz sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Die Ausführungen des Vertreters der Stadt über den Petenten waren jedenfalls für Eingeweihte bzw. Ortskundige personenbeziehbar. Nachdem die Einwilligung des Petenten nicht vorlag und es auch keine andere Rechtsgrundlage gab, hätte sich die Stadt in Anwesenheit eines Pressevertreters und anderer Privatpersonen nicht in dieser Art und Weise äußern dürfen.

Wir hätten es zwar für vertretbar gehalten, dass die Stadt die Presse und damit indirekt die interessierte Leserschaft darüber informiert, warum der neue Radweg an der besagten Stelle nur „provisorischen“ Charakter hat. Die Stadt und das Straßenbauamt hätten sich sonst dem Vorwurf ausgesetzt gesehen, schlechte Arbeit geleistet zu haben. Die Stadt hätte sich aber darauf beschränken müssen, dies sachlich zu begründen. Der städtische Vertreter hätte z. B. darauf hinweisen können, dass die Grunderwerbsverhandlungen in diesem Bereich leider nicht erfolgreich waren. Dagegen waren die Werturteile über den Petenten in Anwesenheit von Dritten durch die Vorschriften des Landesdatenschutzgesetzes nicht gedeckt und damit unzulässig. Wir haben die Stadt gebeten, die datenschutzrechtlichen Vorschriften künftig zu beachten.

### 4. Unzulässige Auskunft aus dem Melderegister

Eine Petentin hat uns folgenden Sachverhalt geschildert: Im Zusammenhang mit einem Mietrechtsstreit habe das Einwohnermeldeamt ihrer früheren Wohngemeinde der Schwiegertochter des Vermieters eine erweiterte Auskunft aus dem Melderegister über den Tag ihres Auszugs aus der Mietwohnung erteilt. Das Einwohnermeldeamt habe sich vom Antragsteller dessen berechtigtes bzw. rechtliches Interesse an der Auskunft nicht nachweisen lassen. Auch eine Vollmacht des Vermieters sei nicht verlangt worden. Ferner habe es das Einwohnermeldeamt versäumt, sie über die erteilte Melderegisterauskunft zu unterrichten. Im Übrigen sei die frühere Wohngemeinde für die Auskunftserteilung gar nicht zuständig gewesen.

Die von uns angehörte Gemeinde hat sich hierzu wie folgt geäußert: Das „besondere rechtliche Interesse“ an der beantragten Melderegisterauskunft und die Bevollmächtigung der Schwiegertochter des Vermieters seien durch Vorlage der Ladung des Vermieters zum Gerichtstermin nachgewiesen worden. Allerdings habe das Einwohnermeldeamt nicht nachgeprüft, ob der Tag des Auszugs der Mieterin für den Rechtsstreit relevant ist. Erfahrungsgemäß sei es aber bei Mietstreitigkeiten in der Regel entscheidungserheblich, wie viele Personen sich zu welchem Zeitpunkt in der Mietsache aufgehalten haben. Die Betroffene sei über die erteilte Melderegisterauskunft nicht unterrichtet worden, weil die Meldebehörde von einem rechtlichen Interesse an der Auskunft ausgegangen sei.

Wir haben den Sachverhalt datenschutzrechtlich wie folgt bewertet: Soweit jemand ein berechtigtes Interesse glaubhaft macht, darf ihm nach § 32 Abs. 2 Satz 1 des Meldegesetzes (MG) zusätzlich zu den Namen und Anschriften eines bestimmten Einwohners eine erweiterte Melderegisterauskunft u. a.

über den Tag des Auszugs erteilt werden. Die Meldebehörde hat den Betroffenen über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten, es sei denn, Letzterer hat ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, glaubhaft gemacht (§ 32 Abs. 2 Satz 4 MG). An die Glaubhaftmachung eines berechtigten Interesses dürfen zwar keine überzogenen Anforderungen gestellt werden. Der Antragsteller muss aber im konkreten Einzelfall sein berechtigtes Interesse an einer bestimmten Melderegisterauskunft gegenüber der Meldebehörde plausibel machen. Diese rechtliche Voraussetzung war im vorliegenden Fall offensichtlich nicht erfüllt. Jedenfalls hätte die Meldebehörde allein aufgrund der Vorlage einer gerichtlichen Ladung die erbetene Melderegisterauskunft nicht erteilen dürfen. Das Vorlegen einer solchen Ladung durch einen Dritten wird auch den Anforderungen an eine ordnungsgemäße Bevollmächtigung nicht gerecht. Insoweit schließen wir uns der Rechtsauffassung der Petentin an. Ich habe den Datenschutzverstoß beanstandet und die Gemeinde gebeten, die datenschutzrechtlichen Vorschriften künftig zu beachten.

Beiden Seiten haben wir ferner mitgeteilt, dass die Eingabe im Übrigen unbegründet war: Ein berechtigtes oder ein rechtliches Interesse im Sinne von § 32 Abs. 2 MG kann im Einzelfall durchaus auch hinsichtlich der personenbezogenen Daten einer Zeugin in einem Zivilprozess zu bejahen sein. Die Melderegisterauskunft darf sich auch auf frühere Einwohner beziehen, wie der Wortlaut des § 32 Abs. 2 Satz 1 Nr. 6 MG („Tag des Auszugs“) belegt. Außerdem sahen wir uns veranlasst, die Petentin darüber aufzuklären, dass privaten Dritten nicht offenbart werden darf, wann die Meldepflicht erfüllt worden ist. Schließlich haben wir ihr mitgeteilt, dass die Meldebehörden nicht verpflichtet sind, derartige Melderegisterauskünfte zu dokumentieren.

## 2. Abschnitt: Personalwesen

### 1. Anschrift „aktualisiert“ – und ab ging die Post an den Falschen

Zwei Jahre, nachdem ein Ministerium den Petenten wegen dauernder Dienstunfähigkeit in den Ruhestand versetzt hatte, wollte es ihn schriftlich zur gesetzlich vorgesehenen amtsärztlichen Nachuntersuchung auffordern. Diese Aufforderung ging dem Petenten allerdings nicht zu. Er erfuhr davon erst durch einen Anruf des Gesundheitsamts.

Das lag daran, dass das Ministerium diese Aufforderung an eine falsche Anschrift gesandt hatte. Obwohl der Petent weiterhin dort wohnte, wohin das Ministerium vor zwei Jahren die Verfügung zur Zurruhesetzung geschickt hatte, verwandte das Ministerium nunmehr eine andere Anschrift. Da unter dieser Anschrift eine gleichnamige Person wohnte, durfte diese davon ausgehen, dass das Schreiben für sie bestimmt war; sie öffnete den Brief daher und konnte so von dem vorzeitigen Ruhestand des Petenten erfahren.

Zur Frage, warum das Ministerium die ihm bekannte, weiterhin richtige Anschrift durch eine falsche ersetzt habe, erklärte es lediglich, die unrichtige Adressierung beruhe auf einem Versehen. Das Ministerium könne nicht mehr nachvollziehen, wie es dazu habe kommen können. Nachdem der Petent seit zwei Jahren nicht mehr aktiv beschäftigt gewesen sei, sei „vorsorglich seine Anschrift auf ihre Aktualität hin überprüft“ worden. Warum und aus welcher Quelle dabei die Anschrift einer gleichnamigen Person übernommen wurde, erklärte das Ministerium nicht. Obwohl das Ministerium mit dem Versand der falsch adressierten Aufforderung an einen Unbeteiligten schwerwiegend in das Recht des Petenten auf informationelle Selbstbestimmung eingegriffen hatte, war in der Stellungnahme des Ministeriums uns gegenüber zu lesen: „Nach unserer Einschätzung liegt kein datenschutzrechtlich relevanter Vorgang vor.“; dies sei hier nicht kommentiert.

Weil die Ausführungen des Ministeriums es nahe legten, dass es dort generell an einem verlässlichen Verfahren fehlte, um Anschriften auf ihre Aktualität hin zu überprüfen, baten wir das Ministerium mitzuteilen, durch welche Maßnahmen es derartige datenschutzrechtliche Verstöße künftig auszuschließen gedenke. Das Ministerium erklärte u. a., wenn es, wie hier, bei Pensionären noch zuständig sei und diese direkt anzuschreiben habe,

werde das Schreiben an die im Personalbogen ausgewiesene Privatanschrift versandt. Sei absehbar, dass das Ministerium ehemalige Beschäftigte anzuschreiben habe, so werde es diese bitten, ihm Adressänderungen unverzüglich mitzuteilen, und gegebenenfalls den Personalbogen aktualisieren. Andere Erkenntnisquellen würden nicht mehr herangezogen. Damit dürfte auch aus unserer Sicht Fällen wie dem geschilderten hinreichend vorgebeugt sein.

**2. Zugriff auf die vollständige Personalakte in Versorgungsfragen**

Ein Landesbeamter teilte uns mit, er habe beim Landesamt für Besoldung und Versorgung Auskunft über die Höhe seiner Versorgungsanwartschaft nach dem Beamtenversorgungsgesetz beantragt. Daraufhin habe das Landesamt ihm zunächst einen Vordruck zugesandt mit der Bitte, diesen ausgefüllt und unterschrieben der für den Petenten zuständigen personalverwaltenden Stelle vorzulegen. Auf diesem Vordruck würde er sich damit einverstanden erklären, dass die personalverwaltende Stelle dem Landesamt seine Personalakte übersende. Das Landesamt habe dazu angeführt, es könne die ruhegehaltsfähigen Dienstzeiten erst dann berechnen, wenn ihm sämtliche erforderlichen Daten vorlägen. Da „wichtige Daten fehlen“ würden, benötige das Landesamt Einsicht in die Personalakte. Ob das rechtens sei, wollte der Petent wissen.

Diese Frage war auf Grundlage der Stellungnahme des Landesamts zu verneinen. Dabei gingen wir mangels gegenteiliger Äußerungen des Landesamts davon aus, dass es für die beantragte Auskunft nicht alle Daten in der Personalakte benötigt hat. Außerdem hätte das Landesamt, wenn es eine Einwilligung des Petenten verlangt, in der Lage sein müssen, die angeblich fehlenden „wichtigen“ Daten näher zu bezeichnen. Das Landesamt stützte sein Vorgehen auf die auf seinem Vordruck erklärte Einwilligung. Zu Unrecht, denn eine solche Erklärung stellte keine wirksame Grundlage für einen Zugriff auf die Personalakte dar.

Zwar ist die Verarbeitung personenbezogener Daten nach § 4 Abs. 1 Nr. 2 LDSG zulässig, soweit der Betroffene eingewilligt hat. Allerdings hat das Landesamt den Umfang der vorgesehenen Einwilligungserklärung mit Blick auf den datenschutzrechtlichen Erforderlichkeitsgrundsatz zumindest auf die Art von Unterlagen zu beschränken, die es jeweils benötigt, um die beantragte Auskunft zu erteilen. Dabei ist insbesondere bedeutsam, dass der Zweck der Personalakte darin besteht, ein möglichst vollständiges Bild über den beruflichen Werdegang und insoweit über die Persönlichkeit des Beamten zu geben. Die vollständige Personalakte kann z. B. Unterlagen über Disziplinarverfahren, dienstliche Beurteilungen und mit dem Dienstverhältnis zusammenhängende Beschwerden enthalten, die das Landesamt für seine Berechnungen sicher nicht benötigt.

Auch wenn das Landesamt die vollständige Personalakte nur deswegen verlangt, damit es dort die für die Auskunft bedeutsamen Angaben heraussuchen kann, erhält es damit die tatsächliche Möglichkeit, auf alle Angaben in der Personalakte zuzugreifen. Die darin liegende Gefährdung des Schutzes personenbezogener Daten ist dadurch auszuschließen, dass das Landesamt nur die Unterlagen zu den fehlenden Daten erbittet und auch nur insoweit eine Einwilligung einholt. Darüber hilft auch nicht hinweg, dass – wie das Landesamt zur Rechtfertigung vorbrachte und was wir nicht bestreiten – heute „auch in der Verwaltung aus betriebswirtschaftlichen Gründen weniger aufwändige, kostengünstige und kundenfreundliche Verfahren praktiziert werden“ müssen. Abgesehen davon, dass das Landesamt zu Aufwand oder Kosten nichts Konkretes sagte, müssen sich auch solche Verfahren im Rahmen der rechtlichen Anforderungen halten. Zum Aufwand, den das Landesamt ins Feld führt, sei hier lediglich angemerkt, dass für bestimmte Unterlagen in der Personalakte ohnehin Teilakten angelegt werden sollen, was einen Zugriff auf einzelne Unterlagen erleichtert.

Auch entspricht die derzeitige Handhabung des Landesamts nicht den Anforderungen des § 4 Abs. 2 LDSG. Danach ist der Betroffene beispielsweise über die beabsichtigte Datenverarbeitung aufzuklären. Dazu sind u. a. die einzelnen Daten zu bezeichnen, die das Landesamt noch benötigt, und die Art der Unterlagen aus der Personalakte zu benennen, auf die sich die Ein-

willigung erstrecken soll. Die Formulierung, dass „wichtige Daten fehlen“, genügt dem nicht. Weiter hat das Landesamt es bisher versäumt, den Antragsteller unter Darlegung der Folgen darauf hinzuweisen, dass er die Einwilligung verweigern kann. Dass die Antragsteller, wie das Landesamt ausführt, „ein gesteigertes Interesse an einer raschen und detailliert richtigen Versorgungsauskunft als Grundlage für ihre weiteren wirtschaftlichen Entscheidungen“ haben, ist keineswegs unvereinbar mit einer rechtmäßigen Handhabung. Um die Auskunft rascher erteilen zu können, sollte das Landesamt in geeigneten Fällen dem Antragsteller die Entscheidung überlassen, ob er dem Landesamt die fehlenden Angaben selbst mitteilt (so dass die personalverwaltende Stelle nicht bemüht zu werden braucht) oder ob er in ein Heranziehen bestimmter Unterlagen aus seiner Personalakte einwilligt.

Wir gehen davon aus, dass das Landesamt die bisherige, unzulässige Handhabung zwischenzeitlich beendet hat. Die von uns erbetene Mitteilung des Landesamts, wie es künftig vorzugehen gedenkt, steht noch aus.

## 3. Abschnitt: Schul- und Hochschulwesen

### 1. Das sog. Nationale Bildungsregister

Das uns schon seit längerem bekannte Vorhaben, in Baden-Württemberg ein komplexes EDV-Verfahren für die Verarbeitung einer Vielzahl personenbezogener Daten von Schülerinnen und Schülern, deren Erziehungsberechtigten sowie Lehrerinnen und Lehrern für Statistik- und Verwaltungszwecke einzuführen, hat inzwischen eine länderübergreifende, bundesweite Dimension erhalten. Individualdaten der Länderdateien sollen zu einer bundesweiten Datenbank zusammengefasst werden.

Mein Amt hatte sich schon wiederholt und intensiv insbesondere mit der vorgesehenen zentralen Erfassung von Individualdaten aller Schülerinnen und Schüler an öffentlichen Schulen in Baden-Württemberg befasst. Zur Vermeidung von Wiederholungen verweise ich auf den Beitrag „Die multifunktionale Schülerindividualdatei: ein Projekt mit vielen Fragezeichen“ in meinem 25. Tätigkeitsbericht (LT-Drs. 13/3800) sowie auf den Beitrag „Zum weiteren rechtlichen Schicksal der Schülerindividualdatei“ in meinem 26. Tätigkeitsbericht (LT-Drs. 13/4910). Im Verlauf dieses Jahres wurde nun bekannt, dass sich die Kultusministerkonferenz u. a. mit „Handlungsempfehlungen für die Datengewinnungsstrategie für die nationale Bildungsberichterstattung“ befasst. Danach ist geplant, einen zentralen Datenpool mit schulstatistischen Einzeldaten einzurichten, in dem ein „Kerndatensatz (KDS) der Länder für schulstatistische Individualdaten“ Verwendung findet. Einer Mitteilung der Kultusministerkonferenz vom Oktober 2006 ist zu entnehmen, dass die Definition des Kerndatensatzes noch nicht abgeschlossen sei, sondern immer noch der laufenden Veränderung unterliege. Nach der hier vorliegenden jüngsten Version dieses Kerndatensatzes ist für Schülerinnen und Schüler, Schulabgänger und Absolventen sowie für Lehrkräfte zwar nicht die Verarbeitung der jeweiligen Namen, dafür aber – neben einer Vielzahl anderer Datenarten – einer Identifikationsnummer vorgesehen. Insbesondere diese Identifikationsnummern geben Anlass für eine sorgfältige datenschutzrechtliche Betrachtung dieses Unterfangens. Individualdaten, die über solche Identifikationsnummern erschlossen werden können, wären zwar pseudonymisiert. Allein damit wäre aber nicht ausgeschlossen, dass die Individualdaten bestimmten Betroffenen zugeordnet werden können. Wenn unter Verwendung der Identifikationsnummern eine solche Zuordnung möglich sein sollte, würde es sich bei den Individualdatensätzen um personenbezogene Daten handeln. Unabhängig von den Identifikationsnummern kann sich ein Personenbezug auch daraus ergeben, dass die Vielzahl und die individuellen Ausprägungen der in einem Datensatz enthaltenen Angaben auf einen bestimmten Betroffenen schließen lassen. Eine länderübergreifende Verarbeitung personenbezogener Daten im Rahmen eines bundesweiten zentralen Datenpools wäre aus datenschutzrechtlicher Sicht in hohem Maße bedenklich. Bislang ist noch nicht einmal klar erkennbar, welchen Zwecken ein Nationales Bildungsregister dienen soll und kann. Schon deshalb lässt sich derzeit nicht ansatzweise erkennen, dass die mit einem solchen Register verbundenen Eingriffe in das Recht Be-

troffener auf informationelle Selbstbestimmung geeignet und erforderlich wären.

Die Kultusministerkonferenz hat ihre Überlegungen noch nicht abgeschlossen. Nach einer Pressemitteilung vom Oktober 2006 hat sie noch keine Festlegungen getroffen; sie hat dabei bekundet, die Belange des Datenschutzes sehr ernst zu nehmen, und daher zu einem öffentlichen Workshop eingeladen, an dem Bildungspolitiker, Bildungswissenschaftler, Datenschützer und Medienvertreter teilnehmen sollen. Anfang Dezember 2006 wird der aktuelle Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an einer Sitzung der Kommission für Statistik der Kultusministerkonferenz teilnehmen, nachdem von dort datenschutzrechtlicher Beratungsbedarf signalisiert worden war.

Wegen der bundesweiten Dimension der Angelegenheit war eine enge Zusammenarbeit der Datenschutzbeauftragten des Bundes und der Länder erforderlich, die auf unserer Konferenz Ende Oktober 2006 in eine entsprechende Entschließung mündete (s. Anhang 6). Inzwischen war zu hören, dass die Schulministerien in mehreren Ländern das bisherige Konzept nicht mehr weiter verfolgen. Es wäre zu begrüßen, wenn das Konzept eines bundesweiten personenbezogenen Datenpools bereits aus diesem Grund ad acta gelegt werden würde.

## 2. Evaluation an Hochschulen

### 2.1 Evaluation von Lehrveranstaltungen

Bereits im vorangegangenen Jahr hatten wir eine Hochschule darüber unterrichtet, dass nach uns vorliegenden Mitteilungen die dortige Evaluation von Lehrveranstaltungen in einem bestimmten Bereich nicht dem Datenschutz entspreche, und um Stellungnahme dazu gebeten. Nachdem diese trotz schriftlicher Erinnerungen auch nach mehr als einem Dreivierteljahr nicht eingegangen war, habe ich diesen Verstoß der Hochschule gegen ihre Unterstützungspflicht gegenüber meinem Amt nach entsprechender Ankündigung beanstandet.

Nach weiteren Rückfragen meines Amts teilte die Hochschule schließlich mit: Es bestehe keine Rechtsgrundlage für die in Rede stehende Evaluation von Lehrveranstaltungen. Jedoch wirke die Hochschulleitung umgehend auf die Verabschiedung einer Evaluationssatzung hin. Auch lägen keine schriftlichen Einwilligungen der Betroffenen vor, wenngleich das Evaluationsverfahren auf der Basis eines Beschlusses des Fakultätsrats erfolgt sei.

Die Evaluation der Lehrveranstaltungen war nach dieser Stellungnahme datenschutzrechtlich unzulässig, denn es lag weder eine entsprechende Hochschulsatzung vor noch hatten die Betroffenen eingewilligt. Der genannte Beschluss des Fakultätsrats konnte, worauf die Hochschule selbst hinwies, Einwilligungen der Betroffenen nicht ersetzen. Diesen datenschutzrechtlichen Verstoß der Hochschule habe ich beanstandet. Zur Absicht der Hochschule, baldmöglichst die erforderlichen Rechtsgrundlagen für die Durchführung von Evaluationen zu schaffen, ist anzumerken, dass hierdurch die datenschutzrechtliche Unzulässigkeit der bereits durchgeführten Evaluationen weder rückwirkend noch für die Zukunft geheilt werden kann.

Die Hochschule fügte ihrer Stellungnahme zu dieser Beanstandung u. a. eine mittlerweile erlassene Evaluationssatzung nach § 5 Abs. 2 des Landeshochschulgesetzes (LHG) bei. Allerdings war für uns nicht erkennbar, dass auf Grundlage dieser Satzung in Verbindung mit § 5 LHG im Rahmen von Evaluationen personenbezogene Daten verarbeitet werden dürfen. Wir haben die Hochschule auf einige noch offene Fragen aufmerksam gemacht. Zudem haben wir unter anderem die Hochschule nochmals darauf hingewiesen, dass personenbezogene Daten ohne entsprechende Rechtsgrundlage nicht weiter gespeichert werden dürfen.

2.2 Personenbezogene Bewertung der Hochschulverwaltung und Weitergabe der Bewertungen

Eine Hochschule wollte erfahren, wie die Studierenden die einzelnen Bereiche der Hochschulverwaltung bewerten. Dazu erbat sie in Fragebögen für jeden Bereich die Bewertung der fachlichen Unterstützung, der Öffnungszeiten, der Qualität und der Quantität der Ausstattung sowie der persönlichen Unterstützung, jeweils auf einer Skala von –2 bis +2. Auf den Fragebögen waren bei den einzelnen Bereichen die dort tätigen Beschäftigten namentlich aufgeführt. Teilweise war lediglich eine Person genannt, etwa beim Studentensekretariat.

Anhand der abgegebenen Fragebögen ermittelte die Hochschule für jeden Bereich sowohl die Durchschnittsbewertung hinsichtlich jeder der fünf Fragen als auch die Gesamtbewertung hinsichtlich aller Fragen. Diese sechs Bewertungen je Bereich teilte die Hochschule den Studierenden und den Beschäftigten mit. Zwar waren bei den Bewertungen die Beschäftigten den Bereichen nicht namentlich zugeordnet, doch konnten die Studierenden und die anderen Beschäftigten, soweit sie mit dem betreffenden Bereich zu tun hatten, ohne weiteres erkennen, auf wen sich die Bewertungen bezogen.

Auf Grundlage der von uns erbetenen Stellungnahme der Hochschule war festzustellen, dass das gewählte Verfahren datenschutzrechtlich unzulässig war. Personenbezogen sind hier jedenfalls diejenigen Daten, die sich auf Bereiche beziehen, in denen lediglich eine Person arbeitet. Die Hochschule berief sich zwar u. a. auf § 5 LHG. Doch diese Vorschrift zur Evaluation bildete keine Rechtsgrundlage für die erfolgte Datenverarbeitung: Abgesehen davon, dass die Hochschule die dort vorgeschriebene Satzung nicht erlassen hatte, diente die Befragung zur Hochschulverwaltung gerade nicht der Bewertung der Arbeit in Forschung und Lehre. Eine andere Rechtsgrundlage war nicht ersichtlich. Schließlich lagen keine Einwilligungen der Betroffenen vor. Ich habe die datenschutzrechtlichen Verstöße der Hochschule beanstandet und sie um Stellungnahme auch dazu gebeten, wie sie eine weitere unzulässige Verarbeitung der personenbezogenen Daten der Beschäftigten ausschließen wolle, auch hinsichtlich der weitergeleiteten Daten. Diese weitere Stellungnahme steht noch aus.

2.3 Weitere Fragen

Das Wissenschaftsministerium bat die Hochschulen des Landes in einem Rundschreiben u. a., alsbald Evaluationssatzungen zu erlassen, um die erforderlichen Rechtsgrundlagen für anstehende Evaluationen nach § 5 LHG zu schaffen. Nachdem das Rundschreiben ausdrückliche Aussagen lediglich zu anstehenden Evaluationen enthielt, nicht jedoch zu bereits durchgeführten oder zumindest begonnenen, wiesen wir das Wissenschaftsministerium darauf hin, dass auch, soweit Hochschulen zum Zeitpunkt des Rundschreibens bereits personenbezogene Daten für Evaluationen verarbeitet hatten, dies nur auf einer entsprechenden Rechtsgrundlage geschehen dürfe. Eventuelle Datenverarbeitungen durch Hochschulen, für die es keine Rechtsgrundlage gebe, seien grundsätzlich unverzüglich zu beenden. Das Wissenschaftsministerium müsse gegebenenfalls die Einhaltung der datenschutzrechtlichen Vorschriften in eigener Verantwortung sicherstellen.

## 3. PISA und andere Vergleichsuntersuchungen an Schulen

In meinem letzten Tätigkeitsbericht hatte ich mit Blick auf die damals anstehenden Untersuchungen der Befragungsreihen PISA (Programme for International Student Assessment) und IGLU (Internationale Grundschul-Lese-Untersuchung) das Problem der unklaren datenschutzrechtlichen Verantwortung angesprochen. Wegen der Einzelheiten verweise ich auf den Beitrag „PISA und IGLU“ in meinem 26. Tätigkeitsbericht (LT-Drs. 13/4910). Damals hatte ich auch meine Erwartung zum Ausdruck gebracht, dass eine Informationsveranstaltung des für die PISA-Studie zuständigen Instituts der Universität Kiel unter Beteiligung von Vertretern der Kultusverwaltungen und der Datenschutzbeauftragten der Länder zur grundlegenden und dauer-

haften Klärung datenschutzrechtlicher Fragen führen könnte. Diese Erwartung hat sich bisher nicht erfüllt. Das mag auch auf den Umstand zurückzuführen sein, dass nicht alle betroffenen Stellen bei dieser Veranstaltung vertreten waren. Mein Amt nutzte die Gelegenheit, im Rahmen dieser Veranstaltung insbesondere die Frage der datenschutzrechtlichen Verantwortung nochmals anzusprechen. Umso erstaunter waren wir, als wir einige Wochen nach dieser Veranstaltung Post vom Kultusministerium erhielten. Dieses übersandte uns wenige Tage vor dem offiziellen Beginn der „PISA 2006-Hauptuntersuchung“ u. a. eine „Prozedurenbeschreibung PISA 2006 Hauptstudie“. Darin war unter der Überschrift „Nationale Projektleitung“ zu lesen, dass „für die Durchführung der Studie in Deutschland ein nationales Konsortium, bestehend aus Wissenschaftlern mehrerer Universitäten und Forschungseinrichtungen unter der Federführung“ eines namentlich benannten Professors einer deutschen Universität, „verantwortlich“ sei. Damit war wiederum nicht klar, wer denn nun für die Verarbeitung personenbezogener Daten verantwortlich ist. Nur der federführende Professor? Oder das Konsortium als solches? Oder die bis auf den federführenden Professor nicht benannten Mitglieder dieses Konsortiums? Die Reihe der Fragen ließe sich fortsetzen. Es schien fast so, als ob die Informationsveranstaltung in Kiel nie stattgefunden hätte und alle Hinweise auf das Erfordernis klarer Aussagen zur datenschutzrechtlichen Verantwortung nicht gefruchtet hätten. Wir haben dem Kultusministerium daraufhin u. a. sogleich mitgeteilt, dass

– die von uns wiederholt angesprochene Frage nach der Verantwortung für die Verarbeitung personenbezogener Daten weiterhin unbeantwortet sei,

– erst nach Klärung dieser Frage eine entsprechende inhaltliche Stellungnahme unsererseits abgegeben werden könne und

– es dem Kultusministerium unbenommen sei, über die Genehmigung der Studie in eigener Verantwortung zu entscheiden.

Danach sind uns keine weitere Mitteilungen in dieser Sache zugegangen. Ich gehe somit davon aus, dass alle datenschutzrechtlichen Fragen und Probleme rechtzeitig vor einer Erhebung oder sonstigen Verarbeitung personenbezogener Daten ausgeräumt wurden. Jedenfalls sind mir keine Anfragen oder Beschwerden von Betroffenen zugegangen.

Derartige Erhebungen an Schulen sind inzwischen auch im Zusammenhang mit einem aktuellen Gesetzgebungsverfahren verstärkt in unseren Blickpunkt geraten. Es handelt sich um den Gesetzentwurf, mit dem ein „§ 114 Evaluation“ in das Schulgesetz eingefügt werden soll. Wegen einer Vielzahl von Unklarheiten der damals aktuellen Fassung des Gesetzentwurfs hatte ich mich in meinem letzten Tätigkeitsbericht auf einige knappe Ausführungen beschränkt. Seither habe ich mich zu diesem Gesetzentwurf noch mehrfach mit dem Kultusministerium ausgetauscht. Um dies gleich vorwegzunehmen: Die datenschutzrechtlich relevanten Probleme konnten leider immer noch nicht mit letzter Klarheit ausgeräumt werden. Deutlich wurde aber Folgendes:

Nach dem Entwurf des § 114 Abs. 2 des Schulgesetzes (im Folgenden: SchG-E) kann das Kultusministerium Schüler und Lehrer verpflichten, an Lernstandserhebungen von internationalen, nationalen oder landesweiten Vergleichsuntersuchungen teilzunehmen, die schulbezogene Tatbestände beinhalten und Zwecken der Schulverwaltung oder der Bildungsplanung dienen. Die Erhebung kann sich dabei auch auf außerschulische Bildungsdeterminanten beziehen, soweit es den Schülern und Lehrern zumutbar ist. Als Beispiel für eine Lernstandserhebung, zu der Schüler und Lehrer demnach verpflichtet werden könnten, wurde uns vom Kultusministerium und von anderer Seite wiederholt die PISA-Studie genannt.

Eine Reihe von Unklarheiten des Gesetzentwurfs konnte bislang nicht ausgeräumt werden. So erklärte mir das Kultusministerium noch Anfang 2006 in einer Besprechung, dass eine Verpflichtung von Schülern und Lehrern nach § 114 Abs. 2 SchG-E nur in Betracht komme, wenn die betroffenen Schüler und Lehrer zuvor jeweils in die freiwillige Teilnahme an Lernstandserhebungen im Sinne des § 114 Abs. 2 SchG-E schriftlich eingewilligt hätten. Dieser – aus datenschutzrechtlicher Sicht wesentliche – Aspekt

kommt in dem später überarbeiteten Gesetzentwurf ebenso wenig zum Ausdruck wie in dem nochmals geänderten aktuellen Gesetzentwurf. Insgesamt stellen sich zum aktuellen Gesetzentwurf vor allem noch zwei gravierende datenschutzrechtliche Fragen:

– Geht es bei den Erhebungen, zu denen das Kultusministerium Schüler und Lehrer verpflichten könnte, überhaupt um personenbezogene Daten? Wenn gar keine Daten mit Personenbezug erhoben werden sollen, sollte dies aus meiner Sicht deutlich im Gesetzentwurf zum Ausdruck gebracht werden. Sofern sich etwa derzeit nicht mit hinlänglicher Sicherheit abschätzen lässt, ob es sich in bestimmten Fällen doch um personenbezogene Daten handelt, wäre beispielsweise an eine gesetzliche Auffangregelung zu denken, wonach personenbezogene Daten nur mit Einwilligung der Betroffenen erhoben werden dürfen.

– Was ist unter dem Begriff „außerschulische Bildungsdeterminanten“ zu verstehen? Oder anders ausgedrückt: Welche Grenzen sind vom Kultusministerium oder anderen (etwa einer für die Durchführung der Erhebung zuständigen Universität) hinsichtlich einer personenbezogenen Datenerhebung zu beachten? Eine klare Antwort auf diese Frage ergibt sich auch nicht aus dem Begründungsteil des Gesetzentwurfs, wonach „außerschulische Bildungsdeterminanten, insbesondere Daten zum sozialen Hintergrund“, nur erhoben werden können, „soweit sie zur Interpretation der Lernstandsergebnisse erforderlich sind“. Diese Frage ist nach meinen Erfahrungen in vergleichbaren Angelegenheiten von außerordentlicher Bedeutung. So war es aus datenschutzrechtlicher Sicht höchst bedenklich, dass nach der Neukonzeption des Sozialministeriums für Einschulungsuntersuchungen die Eltern von Kindergartenkindern zukünftig u. a. gefragt werden sollten, ob es zurzeit gesundheitliche oder andere Probleme in der Familie gibt oder ob in Gegenwart ihres Kindes in der Wohnung geraucht wird. Ich verweise dazu auf den Beitrag „Einschulungsuntersuchungen“ in meinem 26. Tätigkeitsbericht. Entsprechende Probleme, die sich bei solchen Vergleichsuntersuchungen durch eine – für die Betroffenen verpflichtende! – Datenerhebung zum außerschulischen, d. h. unter Umständen privaten, familiären, höchstpersönlichen oder gar intimen Bereich, ergeben könnten, sollten durch eine klare gesetzliche Regelung bereits von vornherein ausgeräumt werden. Die vorgesehene Regelung, dass sich solche Erhebungen nur dann auf außerschulische Bildungsdeterminanten beziehen können, soweit es den Schülern und Lehrern zumutbar ist, lässt nicht erkennen, ob damit auch die berechtigten Interessen der Erziehungsberechtigten der Schüler oder sonstiger Personen im außerschulischen Lebensbereich der Schüler (beispielsweise sonstiger Verwandter oder Bekannter) berücksichtigt werden sollen.

Es ist mir wohl bewusst, dass das Verfahren zur Einführung des § 114 Abs. 2 SchG bereits weit fortgeschritten ist. Gleichwohl würde ich es sehr begrüßen, wenn meine datenschutzrechtlichen Anmerkungen auch „auf der Zielgeraden“ des Gesetzgebungsverfahrens noch Berücksichtigung finden würden. Dadurch könnte es vermieden werden, den Gesetzesvollzug durch Unklarheiten unnötig zu erschweren. Zwar soll das Kultusministerium nach § 114 Abs. 3 SchG-E ermächtigt werden, durch Rechtsverordnung die Themen, die Methoden, das Verfahren und den Zeitpunkt der Evaluationen näher zu regeln. Es ist aus meiner Sicht aber noch nicht klar, ob diese Verordnungsermächtigung auch den Regelungsgegenstand des § 114 Abs. 2 SchG-E erfassen soll. Sollte dies der Fall sein, müssten sich aus § 114 Abs. 2 SchG-E Inhalt, Zweck und Ausmaß der Verordnungsermächtigung mit hinlänglicher Klarheit ergeben. Eine solche Klarheit besteht nach meiner Einschätzung aber gerade nicht.

## 4. Abschnitt: Sonstiges

### 1. Der „Einbürgerungstest“ für Muslime und andere Betroffene

Mitte Dezember des letzten Jahres erfuhr ich aus der Presse, dass in Baden-Württemberg im Januar 2006 eine neue Befragung in Gestalt eines sog. Einbürgerungstests eingeführt werden solle. Das Innenministerium habe einen

Katalog von 30 Fragen, der als Leitfaden dienen solle, erarbeitet. Dieser solle insbesondere bei einer eingehenden Befragung von Muslimen verwendet werden, um herauszufinden, wie sie zur freiheitlichen demokratischen Grundordnung stehen. Schon bisher müssten alle Einbürgerungswilligen ein schriftliches Bekenntnis zur freiheitlichen demokratischen Grundordnung abliefern und Grundkenntnisse in Sachen Demokratie nachweisen. Dem Innenministerium reiche das aber nicht mehr aus.

Mein Amt ging der Sache sogleich nach und bat das Innenministerium um Übersendung der einschlägigen Unterlagen sowie um Information über die beabsichtigte Verarbeitung personenbezogener Daten. Darauf übersandte uns das Innenministerium Anfang Januar 2006 zunächst den sog. Gesprächsleitfaden für die Einbürgerungsbehörden. Dieser enthält unter 30 Gliederungspunkten einen Katalog von Fragen. Der vollständige Gesprächsleitfaden ist in diesem Tätigkeitsbericht als Anhang 11 abgedruckt. Dieser Gesprächsleitfaden hat in den Medien und in der breiten Öffentlichkeit eine lebhafte Diskussion um die Themen Einwanderung, Integration und Dialog der Religionen bzw. Kulturen ausgelöst. Zu jedem dieser Themen ließe sich einiges sagen; ich beschränke mich hier auf die aus meiner Sicht besonders problematischen Fragen des Leitfadens:

„4. Wie stehen Sie zu Kritik an einer Religion? Halten Sie diese für zulässig? Setzen Sie sich damit auseinander?

...

12. In Deutschland kann jeder selbst entscheiden, ob er sich lieber von einem Arzt oder einer Ärztin behandeln lässt. In bestimmten Situationen besteht diese Wahlmöglichkeit jedoch nicht: Notfall, Schichtwechsel im Krankenhaus. Würden Sie sich in einem solchen Fall auch von einer Ärztin (männlicher Einbürgerungsbewerber) oder einem Arzt (Einbürgerungsbewerberin) untersuchen oder operieren lassen?

...

16. Wie stehen Sie dazu, dass Schulkinder an Klassenausflügen und Schullandheimaufenthalten teilnehmen?

...

18. Bei Einbürgerungsbewerberinnen: Ihre Tochter möchte sich gerne so kleiden wie andere deutsche Mädchen und Frauen auch, aber Ihr Mann ist dagegen? Was tun Sie?

...

29. Stellen Sie sich vor, Ihr volljähriger Sohn kommt zu Ihnen und erklärt, er sei homosexuell und möchte gerne mit einem anderen Mann zusammen leben. Wie reagieren Sie?

...

30. In Deutschland haben sich verschiedene Politiker öffentlich als homosexuell bekannt. Was halten Sie davon, dass in Deutschland Homosexuelle öffentliche Ämter bekleiden?“

Im weiteren Verlauf des Januar erhielten wir vom Innenministerium dann zwar noch keine Stellungnahme, dafür aber eine Verwaltungsvorschrift vom 13. September 2005 zur Einführung des Gesprächsleitfadens sowie ein Protokoll über Dienstbesprechungen des Innenministeriums mit den Einbürgerungsbehörden, auf das in dieser Verwaltungsvorschrift „wegen der Einzelheiten des Verfahrens“ Bezug genommen wird. Aus dem Protokoll ergab sich u. a., dass nach Einschätzung des Innenministeriums „generell bei Muslimen“ Zweifel bestehen, ob ein Einbürgerungsbewerber den Inhalt seiner Loyalitätserklärung wirklich verstanden hat und ob sie seiner inneren Überzeugung entspricht. Zudem wird in diesem Protokoll ausgeführt, dass Muslime Staatsangehörige der 57 Mitgliedsstaaten der Islamischen Konferenz seien, es sei denn, die Einbürgerungsbehörde wisse konkret, „dass ein Einbürgerungsbewerber aus einem dieser Staaten kein Muslim ist oder dass er Muslim ist, obwohl er aus einem anderen Staat stammt (z. B. Indien, Bosnien-Herzegowina, Serbien, soweit es sich z. B. um Kosovo-Albaner handelt)“.

Am 20. Januar 2006 musste ich wiederum aus der Presse erfahren, dass das Innenministerium am 17. Januar 2006 – offenkundig um die insbesondere bei Muslimen im In- und Ausland verbreitete Empörung zu dämpfen – einen ergänzenden Erlass zur Anwendung des Gesprächsleitfadens herausgegeben haben soll. Danach bestehe „kein Generalverdacht mehr gegen Muslime“, der neue Erlass bedeute eine „erhebliche Richtungsänderung“ des Innenministeriums. Die intensive Befragung solle nur noch für diejenigen Fälle gelten, bei denen „Zweifel“ am Bekenntnis zur freiheitlichen demokratischen Grundordnung bestünden, und zwar unabhängig von der Nationalität der Bewerber. Noch am selben Tag wandte ich mich an das Innenministerium und äußerte auf der Grundlage der damals vorliegenden, noch unvollständigen Informationen erhebliche Zweifel, ob mit dem vom Innenministerium gewählten Vorgehen ein durchgängig transparentes und faires Einbürgerungsverfahren gewährleistet ist.

Angesichts der wichtigen inhaltlichen Fragen sei hier nur am Rande ein verfahrensrechtlicher Aspekt der Angelegenheit erwähnt: Nach § 31 Abs. 3 Satz 2 LDSG ist mein Amt u. a. bei der Ausarbeitung von Verwaltungsvorschriften zu beteiligen, wenn sie die Verarbeitung personenbezogener Daten betreffen. Das war bei der Verwaltungsvorschrift vom 13. September 2005 sowie bei dem Erlass vom 17. Januar 2006 eindeutig der Fall. Daher habe ich beide Verstöße gegen das datenschutzrechtliche Beteiligungserfordernis noch am 20. Januar 2006 förmlich beanstandet und um kurzfristige Stellungnahme zu dem gesamten Vorgang gebeten.

Das Innenministerium legte mir daraufhin zusammen mit seiner Stellungnahme den Änderungserlass vom 17. Januar 2006 vor. In diesem Erlass war u. a. zu lesen:

> „Wenn der Einbürgerungsbewerber die Bekenntnis- und Loyalitätserklärung abgibt, wird in jedem Fall wie bisher zwangsläufig ein Gespräch mit ihm darüber geführt werden. Stellen sich dabei Zweifel am Verständnis oder an der Wahrhaftigkeit des Bekenntnisses heraus oder werden solche bestätigt, ist das Gespräch anhand des Leitfadens fortzusetzen, um so eine Bewertung der entsprechenden Einbürgerungsvoraussetzung zu ermöglichen. Dabei wird es auch bei Antragstellern aus den 57 der islamischen Konferenz angehörenden Staaten vielfach Einbürgerungsbewerber geben, bei denen die Einbürgerungsbehörde durch das Gespräch oder aufgrund sonstiger Umstände die Überzeugung gewinnt, dass ein weiteres, vertieftes Gespräch unter Verwendung des Gesprächsleitfadens nicht angezeigt ist.“

Meine datenschutzrechtliche Prüfung der Verwaltungsvorschrift(en) ergab insbesondere Folgendes:

– Auf die Anwendung der oben zitierten Fragen Nummern 4, 12, 16, 18, 29 und 30 ist zu verzichten. Denn eine damit verbundene Datenerhebung entspricht nicht dem Erforderlichkeitsgrundsatz des § 13 Abs. 1 LDSG. Nach dieser Vorschrift ist das Erheben personenbezogener Daten (nur dann) zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Hinsichtlich dieser Fragen ist aber, auch unter Würdigung der Äußerungen des Innenministeriums, kein unmittelbarer Bezug zu den Rechten und Grundsätzen erkennbar, die unter dem Begriff der freiheitlichen demokratischen Grundordnung (FDGO) zusammengefasst sind. Es ist nicht ersichtlich, welchen Erkenntniswert Antworten auf diese Fragen für die Prüfung, ob sich ein Ausländer zur FDGO bekennt, haben könnten. Ein Ausländer, der, um ein konkretes Beispiel zu nennen, die Fragen nach Nummer 4 des Gesprächsleitfadens so beantwortet, dass er Kritik an einer Religion ablehnend gegenübersteht, diese nicht für zulässig hält und sich damit nicht auseinandersetzt, würde damit seine vom Grundgesetz geschützte Meinung äußern. Solchen Äußerungen wäre nicht zu entnehmen, ob der Ausländer, was es nach Mitteilung des Innenministeriums festzustellen gilt, „bereit ist, abweichende Meinungen und Lebensweisen anderer zu achten und zu tolerieren“. Hinsichtlich des u. a. vom Begriff der FDGO erfassten Rechts auf freie Entfaltung der Persönlichkeit wäre Antworten auf diese Fragen nur zu entnehmen, wie der jeweilige Ausländer dazu steht. Hinsichtlich des Bekenntnisses des jeweiligen Ausländers zur FDGO wäre den Antworten insoweit aber nichts zu entneh-

men. Auch mit Blick auf die Volkssouveränität, die Gewaltenteilung, die Verantwortlichkeit der Regierung, die Gesetzmäßigkeit der Verwaltung, die Unabhängigkeit der Gerichte, das Mehrparteienprinzip und die Chancengleichheit für alle politischen Parteien mit dem Recht auf verfassungsmäßige Bildung und Ausübung einer Opposition würden sich keine für die Aufgabenerfüllung der Einbürgerungsbehörden erforderlichen Informationen ergeben. Das gilt für die Fragen nach den Nummern 12, 16, 18, 29 und 30 des Gesprächsleitfadens entsprechend, da auch mit diesen Fragen lediglich die Meinung des oder der jeweils Befragten erhoben werden soll. Generell ist anzumerken, dass das bloße „Haben einer Meinung“ so lange keine Gefahr für die freiheitliche demokratische Ordnung darstellt, als es sich nicht in konkreten Handlungen äußert, die gegen diese Ordnung gerichtet sind. Zu Frage Nummer 12 nach der Wahl von Arzt oder Ärztin ist anzumerken: Antworten auf diese Frage können auf den unterschiedlichsten Umständen oder Erwägungen, etwa auch im persönlichen oder intimen Bereich, der Antwortenden beruhen. Auch im Notfall bleibt es jedem unbenommen, sich nach seinen Vorstellungen lieber von einem Arzt oder einer Ärztin behandeln lassen zu wollen. Unter dem Aspekt der „Einstellung des Einbürgerungsbewerbers zur Gleichwertigkeit von Mann und Frau“ lassen sich aus entsprechenden Antworten zu dieser Frage daher keine Erkenntnisse für die Prüfung des Bekenntnisses zur FDGO ableiten. Soweit mit der Frage Nummer 18 die Einstellung einer Einbürgerungsbewerberin zur freien Entfaltung der Persönlichkeit eines Familienangehörigen erhoben werden soll, wäre der Bezug zur FDGO nur mittelbar. Denn die Antworten würden nur das Verhältnis zwischen Privatpersonen betreffen, nicht aber das Verhältnis zwischen Privatpersonen und dem Staat. Die Fragen Nummern 29 und 30 zielen wohl (auch) darauf ab, die Einstellung der oder des Betroffenen zum Recht auf freie Entfaltung der Persönlichkeit anderer in Erfahrung zu bringen. Insofern ist ein Bezug zum Begriff der FDGO ersichtlich. Dennoch begegnet die Erforderlichkeit der Datenerhebung gravierenden Bedenken: Denn ein unmittelbarer Bezug zur FDGO ist ebenso wie bei Frage Nummer 18 nicht gegeben. Zudem können auch Antworten auf diese Fragen, wie bei Frage Nummer 12, auch Gründe im familiären, persönlichen oder intimen Bereich haben. Es gibt keine über die allgemein gebotene Toleranz unterschiedlicher Lebensformen hinausgehende positive Bekenntnispflicht zur Homosexualität. Es bleibt daher jedem unbenommen, in seiner persönlichen Vorstellung für oder gegen ein Zusammenleben gleichgeschlechtlicher Partner oder für oder gegen das Bekleiden öffentlicher Ämter durch Homosexuelle zu sein. In der Regel wird eine Beantwortung der Fragen der Nummern 29 und 30 daher keine Erkenntnisse für die Prüfung des Bekenntnisses zur FDGO liefern können. Demgegenüber besteht vielmehr die Gefahr, in unzulässiger Weise Daten über höchst intime Vorstellungen zum Sexualleben zu erfassen und zu verarbeiten.

– Folgende Unklarheiten zum Anwendungsbereich der Verwaltungsvorschrift sollten ausgeräumt werden:

  Nach den Vorgaben des Innenministeriums soll die mit der Verwaltungsvorschrift vorgesehene Erhebung personenbezogener Daten sowohl bei der sog. Anspruchseinbürgerung nach § 10 Abs. 1 Satz 1 des Staatsangehörigkeitsgesetzes (StAG) wie auch bei der Ermessenseinbürgerung nach § 8 StAG erfolgen. Hinsichtlich der Erfüllung der Aufgaben der Einbürgerungsbehörden im Sinne des § 13 Abs. 1 LDSG ist demnach zu unterscheiden:

  Bei der Prüfung, ob ein Rechtsanspruch auf Einbürgerung besteht, haben die Einbürgerungsbehörden u. a. § 10 Abs. 1 Satz 1 Nr. 1 StAG zu beachten. Danach gehört es zu den dort ausdrücklich genannten Voraussetzungen für einen Einbürgerungsanspruch eines Ausländers, dass sich dieser zur freiheitlichen demokratischen Grundordnung des Grundgesetzes für die Bundesrepublik Deutschland bekennt. Es ist aus datenschutzrechtlicher Sicht unter Berücksichtigung verwaltungsgerichtlicher Rechtsprechung nicht zu beanstanden, wenn das demnach erforderliche Bekenntnis zur FDGO nicht nur als rein formelle Einbürgerungsvoraussetzung betrachtet wird, sondern die Einbürgerungsbehörden gegebenenfalls der Frage nachgehen, ob ein solches Bekenntnis auch inhaltlich zutrifft.

Allerdings müssen objektive Anhaltspunkte vorliegen, um das vom Einbürgerungsbewerber abgegebene Bekenntnis zur FDGO in Frage stellen zu können. Ob und inwieweit diese Anhaltspunkte bereits vor Beginn des Gesprächs vorliegen müssen, ist nicht zweifelsfrei geregelt. Hierfür spricht, dass nach dem Protokoll, das zum Bestandteil der Verwaltungsvorschrift gemacht worden ist, das Gespräch anhand des Leitfadens immer dann (gemeint ist damit offenbar auch: nur dann) geführt werden soll, wenn die Einbürgerungsbehörde Zweifel an der inneren Hinwendung des Bewerbers zur Werteordnung der Bundesrepublik Deutschland – also an der Übereinstimmung von äußerlichem Bekenntnis und innerer Einstellung – hat. Zweifel können danach nur dann vorliegen, wenn sie bereits vor Beginn des Gesprächs durch tatsächliche Anhaltspunkte in der Person bzw. im Verhalten des Einbürgerungsbewerbers geweckt worden sind. Demgegenüber zielt die Verwaltungsvorschrift des Innenministeriums darauf ab, „Regelvermutungen“ für Zweifel – wie etwa Religionszugehörigkeit zum Islam, festgemacht an der Herkunft des Bewerbers aus einem Mitgliedstaat der Islamischen Konferenz – aufzustellen, die dann vom Bewerber in dem Gespräch quasi widerlegt werden müssen. Ein „Schönheitsfehler“ der Regelvermutung war zudem, dass in einigen Mitgliedstaaten der Islamischen Konferenz die Muslime nicht die Mehrheit in der Bevölkerung ausmachen. Die Herkunft des Bewerbers aus einem dieser – insbesondere afrikanischen – Staaten war also kein Beleg dafür, dass er selbst Muslim ist.

Bei der Prüfung, ob ein Ausländer nach § 8 StAG eingebürgert werden kann, ist indessen zu berücksichtigen, dass das Bekenntnis des Einbürgerungsbewerbers zur FDGO, anders als in den Fällen des § 10 Abs. 1 Satz 1 StAG, nicht zu den in § 8 StAG ausdrücklich genannten tatbestandlichen Voraussetzungen zählt. Es ist somit fraglich, ob Einbürgerungsbehörden bei einer Ermessenseinbürgerung nach § 8 StAG in identischer Weise wie bei einer Anspruchseinbürgerung nach § 10 StAG prüfen dürfen, ob sich ein betroffener Ausländer zur FDGO bekennt. Zwar soll nach der Verwaltungsvorschrift des Innenministeriums zum Staatsangehörigkeitsgesetz vom 5. Januar 2001 die Voraussetzung der Abgabe eines Bekenntnisses zur FDGO „in gleicher Weise auch bei der Ermessenseinbürgerung“ gelten. Mit diesem undifferenzierten Hinweis in einer Verwaltungsvorschrift kann jedoch die für Anspruchseinbürgerung und Ermessenseinbürgerung deutlich unterschiedliche gesetzliche Ausgangslage nicht einfach eingeebnet und gleichgeschaltet werden. Das nach § 8 StAG vorgesehene Ermessen verlangt vielmehr differenziertere Erwägungen der Einbürgerungsbehörden.

Zur eindeutigen Klärung, welche Daten für den Nachweis des Bekenntnisses zur FDGO verarbeitet werden dürfen (insbesondere welche besonders sensiblen personenbezogenen Daten), empfiehlt sich nach meiner Einschätzung eine ausdrückliche bundesgesetzliche Regelung. Schließlich geht es bei der Einbürgerung nicht um die Verleihung einer baden-württembergischen oder hessischen, sondern der deutschen Staatsangehörigkeit; insofern stellt sich bereits aus diesem Grund die Frage, inwieweit die Bundesländer eigene und unterschiedliche Anforderungen an den Erwerb der deutschen Staatsangehörigkeit stellen dürfen.

Das Innenministerium teilte mir in einem weiteren Schreiben mit, dass es meine kritische Beurteilung der oben zitierten Fragen nicht teile. Allerdings ist mir auf anderem Wege bekannt geworden, dass eine Überprüfung des Gesprächsleitfadens erfolgen soll. In der LT-Drucksache 14/22 wies das Justizministerium im Einvernehmen mit dem Innenministerium auf Folgendes hin:

„Zudem hat die Landesregierung im Koalitionsvertrag die Überprüfung des Einbürgerungsleitfadens vereinbart. Dabei wird insbesondere die Frage zu klären sein, ob der Gesprächsleitfaden in allen Punkten geeignet ist, den Einbürgerungsbehörden als Hilfsmittel zu dienen.“

Ich teilte dem Innenministerium mit, dass ich eine solche Überprüfung ausdrücklich begrüße. Zudem bat ich um die Beteiligung meines Amts im Verfahren zur Überprüfung des Gesprächsleitfadens. Bislang habe ich dazu noch keine Rückmeldung erhalten. Vor wenigen Wochen konnte ich im-

merhin der Presse entnehmen, dass der Leitfaden bis Ende des Jahres abschließend überarbeitet sein solle und das Innenministerium demnächst dem Integrationsbeauftragten der Landesregierung Verbesserungsvorschläge machen wolle. Auch die Innenministerkonferenz hat inzwischen einheitliche Einbürgerungsstandards verabschiedet; ein entsprechender Gesetzesvorschlag für den Bundesrat ist in Arbeit. Ich gehe davon aus, dass einer Beteiligung meines Amts nach § 31 Abs. 3 Satz 2 LDSG an einer Nachbesserung des Einbürgerungsverfahrens diesmal nichts im Wege stehen wird.

Unmittelbar vor Redaktionsschluss für diesen Tätigkeitsbericht war zu erfahren, dass die Innenministerkonferenz den Gedanken an eine bundesgesetzliche Regelung nun offenbar konkret aufgreift. Nach einer Veröffentlichung der Geschäftsstelle der Innenministerkonferenz haben die Innenminister und -senatoren auf ihrer Sitzung im November 2006 einen Gesetzesvorschlag zur Umsetzung bundeseinheitlicher Einbürgerungsstandards zustimmend zur Kenntnis genommen. Der Gesetzesvorschlag, der vom Freistaat Bayern zusammen mit dem Land Baden-Württemberg und anderen Bundesländern in den Bundesrat eingebracht werden soll, sieht vielfältige Änderungen des Staatsangehörigkeitsgesetzes vor. Dabei soll z. B. nach einem neuen § 11 Abs. 1 Nr. 1 StAG eine Einbürgerung ausgeschlossen sein, „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass das Bekenntnis des Ausländers zur freiheitlichen demokratischen Grundordnung des Grundgesetzes für die Bundesrepublik Deutschland nicht glaubwürdig ist, und diese auch in einem Gespräch nicht ausgeräumt werden können“. Dieser Ansatz einer bundesgesetzlichen Regelung ist – wie bereits erwähnt – grundsätzlich zu begrüßen. Allerdings müsste der Gesetzentwurf, wenn er denn eingebracht ist und vollständig vorliegt, auch datenschutzrechtlich noch eingehend geprüft werden.

## 2. Zu viele Daten bei Postzustellung und Nachforschungsauftrag

Bei einem Nachforschungsauftrag habe es die Post nicht zu interessieren, welche Angelegenheit das zuzustellende Schreiben betroffen hat, fand der Adressat eines solchen Schreibens. Dem lag zugrunde, dass ein Landratsamt an den Petenten ein Schreiben mit Postzustellungsurkunde versandt hatte, diese jedoch nicht zurückkam. Deswegen bat das Landratsamt die Post schriftlich um Mitteilung, ob und wann das Schreiben zugestellt worden sei. Dabei gab das Landratsamt an, dass es um ein Ordnungswidrigkeitenverfahren gegen den Petenten ging, nannte als zuständige Stelle den Fachbereich Zentrale Bußgeldangelegenheiten und führte zudem dessen E-Mail-Adresse mit der Postfachbezeichnung „bußgeldstelle“ auf.

Das Landratsamt führte in seiner von uns erbetenen Stellungnahme aus, die im Briefkopf verwandte Bezeichnung Zentrale Bußgeldstelle sei die amtliche Bezeichnung für diesen Fachbereich des Landratsamts. Sie werde in jedem Schreiben der Behörde genannt. Es sehe darin keinen Anhaltspunkt für die Post, auf den Inhalt zu schließen, was ja auch für Schreiben der Gerichte, Finanzämter und anderer Dienststellen gelte. In seiner Stellungnahme kündigte das Landratsamt ferner an, künftig bei Nachforschungsaufträgen an die Post nur noch auf den Adressaten und „die Zustellung“ (die Angaben, welche die Post für die Nachforschung benötigt) Bezug zu nehmen. Wir bewerteten den Vorgang wie folgt:

– Postzustellung

  Ob die Bezeichnung Zentrale Bußgeldstelle auf dem zuzustellenden Schreiben selbst aufgeführt wird, ist datenschutzrechtlich belanglos, weil es in einem verschlossenen Umschlag zuzustellen ist. Auf dem Umschlag dagegen darf eine solche Bezeichnung nicht erscheinen. Das gilt unabhängig davon, ob daraus zu schließen ist, dass der Adressat Betroffener ist (also ihm vorgeworfen wird, eine Ordnungswidrigkeit begangen zu haben). Absenderangabe und Aktenzeichen sollen bei der Zustellung durch die Post mit Zustellungsurkunde keine Zusätze enthalten, die Rückschlüsse auf den Inhalt des Schreibens zulassen. Dies ist in Nummer 2.1.1 der Verwaltungsvorschrift des Innenministeriums zum Landesverwaltungszustellungsgesetz klargestellt. Als Beispiele sind dort genannt: „Bußgeldstelle“ und „Az.: OWi ...“. Für den Fall, dass eine weitere

Kennzeichnung erforderlich ist, beispielsweise weil an einem Tag mehrere Entscheidungen unter demselben Aktenzeichen zugestellt werden, ist auch diese weitere Kennzeichnung nach der Verwaltungsvorschrift aus Gründen des Datenschutzes neutral zu halten. Beispielsweise seien die Angaben „Ausweisungsverfügung“ oder „Rückforderung von Sozialhilfe“ zu vermeiden und stattdessen die Angaben „Bescheid“ oder „Verfügung“ zu verwenden.

– Nachforschungsauftrag

Die Angabe, dass es um ein Bußgeldverfahren gegen den Petenten ging, war datenschutzrechtlich unzulässig. Selbstverständlich war es dem Landratsamt allerdings erlaubt, die Post aufzufordern, dem Verbleib des zuzustellenden Schreibens und der Postzustellungsurkunde nachzugehen. Allerdings durfte das Landratsamt der Post dazu ausschließlich diejenigen personenbezogenen Daten mitteilen, welche sie für ihre Nachforschungen benötigt. Das ergibt sich mangels einschlägiger besonderer Rechtsvorschriften aus dem Erforderlichkeitsgrundsatz, der immanenter Bestandteil der Übermittlungsregelungen des Landesdatenschutzgesetzes ist. Datenschutzrechtlich unzulässig war weiter, dass das Landratsamt im Nachforschungsauftrag die Zentrale Bußgeldstelle und die E-Mail-Adresse mit der Postfachbezeichnung „bußgeldstelle“ genannt hatte, denn die Anforderungen an die Absenderangabe bei einer Zustellung sind auch bei Nachforschungsaufträgen heranzuziehen.

### 3. Verkehrsordnungswidrigkeiten: Mitteilung von Fahrerdaten an den Fahrzeughalter

Wer mit einem fremden Kraftfahrzeug eine Verkehrsordnungswidrigkeit begeht, muss damit rechnen, dass die Bußgeldbehörde dem Halter neben dem Zeitpunkt der Tat auch den Tatort, den Tatvorwurf und etwaige Beweismittel mitteilt. Das betrifft insbesondere Fälle, in denen die Bußgeldbehörde den Namen des Täters nicht kennt, weil ihr lediglich das Kennzeichen des Fahrzeugs bekannt ist und gegebenenfalls ein Lichtbild des Fahrers vorliegt, der Halter als Täter aber ausscheidet. Letzteres ist etwa der Fall, wenn die Bußgeldbehörde nach einer Halterabfrage beim Fahrzeugregister feststellt, dass das Fahrzeug auf eine Gesellschaft mit beschränkter Haftung oder, wenn der Fahrer ein Mann war, auf eine Frau zugelassen ist.

Um den Fahrer zu ermitteln, darf die Bußgeldbehörde dem Halter einen Zeugenfragebogen zusenden. Dass sie dabei stets neben dem Zeitpunkt der Tat auch den Tatort, den Tatvorwurf und etwaige Beweismittel mitteilt, wie vom Innenministerium Baden-Württemberg veranlasst, halten wir aus datenschutzrechtlicher Sicht für bedenklich. Im Normalfall genügt der Zeitpunkt der Tat, damit der Halter sich dazu äußern kann, wem er damals sein Fahrzeug überlassen hatte (Unternehmen beispielsweise anhand von Einträgen in ein Fahrtenbuch). Darüber hinausgehende Angaben, etwa zum Tatort oder zum Tatvorwurf, sind dazu regelmäßig nicht nötig. Deren Übermittlung ist deswegen nicht erforderlich. Lediglich wenn der Halter erklärt, er könne das alleine anhand des Zeitpunkts der Tat nicht feststellen, kann es im Einzelfall erforderlich werden, dem Halter zusätzliche Angaben mitzuteilen. Diese Angaben können dazu beitragen, die Ordnungswidrigkeit aufzuklären, wenn der Halter beispielsweise weiß, wer mit seinem Fahrzeug üblicherweise wohin fährt oder wer dazu neigt, Geschwindigkeitsbeschränkungen zu „übersehen“.

Im Verwarnungsgeldbereich (wenn lediglich ein Verwarnungsgeld bis zu 35 € erhoben wird) nannten die Bußgeldbehörden trotz unserer Kritik auf dem Zeugenfragebogen für den Halter bereits bisher stets auch Tatort, Tatvorwurf und etwaige Beweismittel. Das Innenministerium beabsichtigte, diese Handhabung auf alle Bußgeldverfahren auszudehnen. Es teilte uns dazu u. a. mit, Bürger und Unternehmen hätten es immer wieder bemängelt, wenn ihnen lediglich der Zeitpunkt der Tat mitgeteilt worden sei. Insbesondere Unternehmen hätten deswegen häufig zurückgefragt. Der Ombudsmann für Bürokratieabbau im Staatsministerium vertrete die Auffassung, dass – trotz der hoch zu bewertenden Belange des Datenschutzes – durch die Mitteilung aller Angaben bereits im Zeugenfragebogen unnötige Büro-

kratie vermieden werden könne. In anderen Bundesländern erhalte der Halter mit dem Zeugenfragebogen immer alle Informationen; hier bestünden offensichtlich unterschiedliche Bewertungen aus Sicht des Datenschutzes. Das Innenministerium bat uns auch vor diesem Hintergrund, unsere bisherige Auffassung zu überdenken.

In Anbetracht dessen wandten wir uns an die anderen Landesdatenschutzbeauftragten. Diejenigen, die sich dazu äußerten, machten keine Bedenken dagegen geltend, den Halter stets auch über Tatort und Tatvorwurf zu unterrichten. Wir teilten dem Innenministerium deswegen mit, dass wir mit Blick darauf die von ihm bevorzugte Handhabung für vertretbar – wenngleich aus den angeführten Gründen weiterhin für wenig überzeugend – halten. Zugleich empfahlen wir dem Innenministerium, in den Zeugenfragebogen für den Halter weiterhin nicht stets alle Angaben zur Verkehrsordnungswidrigkeit und damit zum Fahrer aufzunehmen.

Das Innenministerium erklärte, unter Abwägung aller Gesichtspunkte wolle es den Wünschen der Bußgeldbehörden und nicht zuletzt der Betroffenen entsprechen, auch im Hinblick auf die politisch gewünschten Ziele „Bürokratieabbau/effiziente Verfahrensabläufe“. Es hat veranlasst, dass dem Fahrzeughalter im Zeugenfragebogen künftig stets auch Tatort und Tatvorwurf nebst etwaigen Beweismitteln eröffnet werden. Wenn die Fahrer fremder Fahrzeuge sich auch deswegen bemühen, die Verkehrsvorschriften einzuhalten, so wäre damit, wenn schon nicht dem Datenschutz, so doch wenigstens der Verkehrssicherheit gedient.

### 4. Die aufschlussreiche Angrenzerbenachrichtigung

Auch der handelsübliche Vordruck eines Formularverlags entspricht nicht zwangsläufig den Vorschriften des Datenschutzes und entbindet die öffentliche Stelle, die diesen verwendet, nicht von der Prüfung der Zulässigkeit der darauf vorgesehenen Datenverarbeitungen und der Verantwortung für diese. Diese Erfahrung musste eine Gemeinde machen, die ein Formblatt eines Formularverlags für Angrenzerbenachrichtigungen im Baugenehmigungsverfahren verwendete:

In der Landesbauordnung ist vorgesehen, dass die Gemeinde die Eigentümer angrenzender Grundstücke von einem Bauantrag zu benachrichtigen hat. Ein Bürger, der eine solche Angrenzerbenachrichtigung erhalten hatte, wandte sich an unsere Dienststelle, weil auf dieser die Namen und Anschriften auch aller weiteren Angrenzer vermerkt waren. Der Bürger ging daher – wie sich später herausstellte, zu Recht – davon aus, dass die Gemeinde auch den anderen Angrenzern seine Anschrift mitgeteilt hatte. Dies ärgerte ihn, der schon vor längerer Zeit aus der Gegend weggezogen war, aus zweierlei Gründen: Erstens hielt er die Weitergabe seiner privaten Wohnanschrift an die übrigen Angrenzer für nicht erforderlich. Zweitens sei er gar nicht (mehr) Eigentümer des angrenzenden Grundstücks, da er dieses in der Zwischenzeit veräußert habe; insofern hätte er gar keine Angrenzerbenachrichtigung erhalten dürfen.

Die um Stellungnahme gebetene Gemeinde verwies auf das handelsübliche Formblatt für Angrenzerbenachrichtigungen im Baugenehmigungsverfahren, auf dem vorgesehen ist, dass alle angrenzenden Eigentümer mit Name, Anschrift und Flurstücksnummer eingetragen werden. Der jeweilige Adressat der Angrenzerbenachrichtigung werde entsprechend den Vorgaben des Formblatts rot angekreuzt. Eine Erforderlichkeit für dieses Vorgehen konnte jedoch weder die Gemeinde selbst noch das von dieser um Stellungnahme gebetene Rechts- und Kommunalamt des Landratsamts darlegen. Letzteres regte daher an, die bisherige Praxis zu ändern und künftig im Rahmen der Angrenzerbenachrichtigung jeden Angrenzer einzeln und ohne Nennung von Namen und Anschriften der übrigen Angrenzer anzuschreiben. Dieser Empfehlung an die betroffene Gemeinde, die schon signalisiert hatte, ihre diesbezügliche Praxis umzustellen, konnten wir uns nur anschließen.

### 5. Das ungepflegte Grab aus Sicht des Datenschutzes

Inwieweit bei Daten Verstorbener noch eine Verpflichtung zu deren Schutz besteht, ist nicht immer ganz einfach zu beantworten. Die Fragestellung,

mit der sich eine städtische Friedhofsverwaltung an uns wandte, bezog sich aber auf Daten Lebender und damit zweifelsohne auf personenbezogene Daten. Es ging um folgendes Problem: Vielfach würden Gräber von den jeweiligen Nutzungsberechtigten nicht gepflegt. Hierüber beschwerten sich oftmals die Nutzungsberechtigten des Nachbargrabs. Daher erhalte der Friedhof zahlreiche Anfragen, in denen um Mitteilung von Name und Adresse des Nutzungsberechtigten des ungepflegten Grabs gebeten werde. Die Friedhofsverwaltung wollte nun wissen, ob sie die Adressdaten weitergeben darf. Ergänzend wurde uns mitgeteilt, dass die Nutzungsberechtigten der ungepflegten Gräber ohnehin von der Friedhofsverwaltung angeschrieben und unter Androhung des Entzugs des Nutzungsrechts um Einhaltung der Pflegevorschriften gebeten werden. Es komme aber auch vor, dass aus Sicht der Nachbarn ein Grab ungepflegt sei, die Friedhofsverwaltung dies aber nicht so sehe. Die Friedhofsverwaltung ging davon aus, dass der Nachbar die Adressdaten des Nutzungsberechtigten des aus seiner Sicht ungepflegten Grabes dazu verwenden wollte, um diesen schriftlich um Abhilfe zu bitten.

Vorliegend war eine Güterabwägung zwischen den Interessen des Nutzungsberechtigten des ungepflegten Grabs und den Interessen des Nutzungsberechtigten des Nachbargrabs vorzunehmen. Folgende Aspekte waren bei dieser Abwägung von Bedeutung: Aufgrund der Tatsache, dass die Friedhofsverwaltung den Nutzungsberechtigten, der sein Grab vernachlässigt, selbst anschreibt und unter Androhung der Aufhebung des Grabnutzungsrechts um Abhilfe bittet, war das Interesse der Nutzungsberechtigten des Nachbargrabs, den Nutzungsberechtigen des vernachlässigten Grabs zusätzlich anzuschreiben, als eher gering zu betrachten. Auch für den Fall, dass sich ein Nutzungsberechtigter durch ein vermeintlich ungepflegtes Grab gestört fühlt, aus Sicht der Friedhofsverwaltung aber keine Vernachlässigung der Grabpflege vorliegt und dieses daher keine Veranlassung sieht, den Nutzungsberechtigten anzuschreiben, war aufgrund des geringen Grads der Störung, die von dem eventuell nicht perfekt gepflegten Grab ausgeht, das Interesse des Nutzungsberechtigten des benachbarten Grabs an der Kenntnis der Adressdaten als nicht sehr groß anzusehen.

Auf der anderen Seite ist zu bedenken, dass es nicht jedem Bürger gleichgültig sein muss, ob ein privater Dritter von seinem Namen und seiner Anschrift im Zusammenhang mit der Nutzungsberechtigung eines Grabs Kenntnis erlangt und er infolgedessen Post von diesem erhält. Daher war aus unserer Sicht das Interesse des Nutzungsberechtigten des angeblich oder tatsächlich ungepflegten Grabs am Ausschluss der Übermittlung grundsätzlich höher zu bewerten als das Interesse des Nutzungsberechtigten des benachbarten Grabes an der Kenntnis dieser Daten. Zu einem anderen Ergebnis kann man kommen, wenn der Nutzungsberechtigte des benachbarten Grabs entsprechende Tatsachen glaubhaft darlegt, aus denen sich ergibt, dass er zivilrechtliche Ansprüche gegen den Nutzungsberechtigten des ungepflegten Grabs geltend machen kann. Eine lediglich optische Beeinträchtigung dürfte hierfür aber nicht ausreichen.

## 5. Teil: Technik und Organisation

### 1. Datenschutz und Datensicherheit in Verwaltungsnetzen

Gab es bis vor einigen Jahren im Bereich der Landesverwaltung nur das im Wege des Outsourcings betriebene Landesverwaltungsnetz (LVN), so wird dies heute ergänzt durch eine wachsende Zahl der im sog. Metronetzverbund zusammengeschlossenen Verbindungen, die von der Landesverwaltung selbst administriert werden. Dieser Wandel sowie der Wunsch, andere Übertragungstechniken zu nutzen, machten eine Fortschreibung der Datenschutz- und Sicherheitskonzeptionen für diese Netze erforderlich.

1.1 Datenschutz- und Sicherheitskonzeptionen für das Landesverwaltungsnetz und den Metronetzverbund

Die uns vom Innenministerium übersandten Entwürfe der Datenschutz- und Sicherheitskonzeptionen für das Landesverwaltungsnetz und den Metronetzverbund gaben Anlass, u. a. auf Folgendes hinzuweisen:

1.1.1 Verschlüsselung der übertragenen Daten

Für das Landesverwaltungsnetz und den Metronetzverbund ist bislang keine generelle Verschlüsselung der darin übertragenen Daten vorgesehen. Daher ist für jede einzelne Anwendung zu prüfen, ob zum Schutz der dabei übertragenen Daten auch deren Verschlüsselung zu realisieren ist. Dies ist aus unserer Sicht zumindest immer dann geboten, wenn besonders schutzbedürftige Daten übertragen werden. Leider gibt es immer wieder Fälle, in denen die Verständigung über die im Einzelfall erforderlichen Sicherheitsmaßnahmen nur sehr schleppend vorankommt.

Ein Beispiel hierfür ist die zwischen dem Innenministerium und unserer Dienststelle bereits seit längerem geführte Erörterung darüber, ob Daten über Sicherheitsbefragungen von Ausländern bei deren Übertragung über das LVN zu verschlüsseln sind. Ein Grund für das Auftreten derartiger Schwierigkeiten mag auch darin liegen, dass die für die Realisierung einzelner Fachverfahren zuständigen Organisationseinheiten vielfach nicht im Detail mit den sicherheitsrelevanten Vereinbarungen über die Sicherheit in den Verwaltungsnetzen vertraut sind und davon ausgehen, dass darüber ohne weiteres auch besonders schutzbedürftige Daten übertragen werden können.

Diese Schwierigkeiten ließen sich umgehen, wenn eine generelle Verschlüsselung der im LVN sowie im Metronetzverbund übertragenen Daten vorgesehen würde. Für eine solche generelle Verschlüsselung sprechen auch noch weitere Argumente:

Auch im Bereich der Verwaltungsnetze ist festzustellen, dass deren Organisation und Technik immer heterogener wird. Dies zeigt sich beispielsweise darin, dass die Landesverwaltung neben dem im Wege des Outsourcings betriebenen LVN zunehmend auch die vom Landesrechenzentrum IZLBW betriebenen Metronetzverbindungen nutzt und darin immer mehr unterschiedliche Übertragungstechniken mit jeweils eigenen Sicherheitsaspekten zum Einsatz kommen sollen.

Hinzu kommt, dass nach dem Aufbau bundesweiter Kommunikationsnetze zahlreiche neue IuK-Verfahren in Betrieb genommen wurden, mit deren Hilfe immer mehr sensible personenbezogene Daten über diese Netzwerke übertragen werden. Nur als Beispiele für diese Entwicklungen sei auf die Vorhaben

- elektronische Steuererklärung, elektronische Lohnsteuerbescheinigungen (Projekt ELSTER),
- Teilnahme an der bundesweiten Nutzung des Informationsaustauschs unter Steuerverwaltungen und Banken (Verfahren LUNA, Kontendatenabrufverfahren),

– Datenübermittlungen im Einwohnermeldewesen,

– Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt,

– elektronische Auskunfts- und Mitteilungsverfahren der Justiz sowie die

– Abwicklung des Haushaltsmanagements (in dem zum Teil auch sehr sensible Daten verarbeitet werden, beispielsweise über Disziplinarstrafen oder über die Abwicklung von Zahlungen, aus denen besondere soziale Notlagen oder Erkrankungen der Zahlungsempfänger hervorgehen)

verwiesen.

Die Realisierung von IuK-Betriebsmodellen, bei denen die von einer Dienststelle genutzten Datei- oder E-Mail-Server nicht mehr als Teil des jeweiligen lokalen Netzes, sondern an zentralen (Rechenzentrums-)Standorten betrieben werden, führt zudem dazu, dass zunehmend auch rein dienststelleninterne Kommunikation den Bereich des örtlichen lokalen Netzwerks verlässt und über Weitverkehrsnetze wie das Landesverwaltungsnetz oder den Metronetzverbund geführt wird.

Angesichts der geschilderten Entwicklungen und der bisherigen Erfahrungen mit der Realisierung kryptografischer Verfahren halten wir es für angebracht, die in Verwaltungsnetzen übertragenen Daten künftig standardmäßig zu verschlüsseln.

Während andernorts mit der Einführung einer solchen flächendeckenden Verschlüsselung bereits Ernst gemacht wird, hinkt Baden-Württemberg in diesem Punkt noch hinterher.

– In Rheinland-Pfalz werden sämtliche über das Landesnetz übertragenen Daten durch eine sog. Leitungsverschlüsselung gesichert.

– Gleiches gilt für das TESTA-Netz, das u. a. die Verwaltungsnetze des Bundes und der Länder verbindet.

– Schließlich sieht auch die „IuK-Landesstrategie für die bayerische Staatsverwaltung“ die Verschlüsselung sämtlicher über das Bayerische Behördennetz übertragenen Daten vor. Der Leitungsverschlüsselung kommt dabei die Aufgabe zu, einen „kryptografischen Grundschutz“ zu leisten. Zum Schutz der Übertragung besonders schutzbedürftiger Daten, wie z. B. Personal- oder Sozialdaten, sieht die IuK-Landesstrategie darüber hinaus die Realisierung einer sog. Ende-zu-Ende-Verschlüsselung vor.

Eine derartige, nach dem Schutzbedarf der Daten abgestufte Konzeption für die Verschlüsselung aller übertragenen Daten stellt aus unserer Sicht ein geeignetes Modell zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität der in den hiesigen Verwaltungsnetzen übertragenen Daten dar. Erfreulicherweise signalisierte das federführende Innenministerium mittlerweile in einem Gespräch die Bereitschaft, eine generelle Verschlüsselung der im LVN und dem Metronetzverbund übertragenen Daten als strategisches Ziel anzuerkennen.

1.1.2 Grundsatz der Datensparsamkeit bei der Netzwerkgestaltung

Sowohl der im Landesdatenschutzgesetz verankerte Grundsatz der Datensparsamkeit als auch die gesetzlichen Anforderungen an technische und organisatorische Schutzmaßnahmen zielen darauf ab, informationstechnische Systeme so zu gestalten, dass personenbezogene Daten damit nur in dienstlich erforderlichem Umfang verarbeitet werden können. Hinsichtlich der Gestaltung von Kommunikationsnetzen und deren Schnittstellen bedeutet dies, dass auch die durch diese eröffneten Kommunikationsmöglich-

keiten stets auf das erforderliche Maß zu begrenzen sind. Da dieser Grundsatz bislang nicht in der notwendigen Klarheit in den vorgelegten Entwürfen berücksichtigt wurde, baten wir um entsprechende Verdeutlichung und Berücksichtigung dieses Grundsatzes.

1.1.3 Einvernehmliche Fortentwicklung der Konzeptionen

Ein Datenschutz- und Sicherheitskonzept muss die zu ergreifenden Maßnahmen möglichst konkret benennen. Die rasche Weiterentwicklung der Technik macht es dabei nötig, dass diese Konzepte auch innerhalb der Laufzeit der Outsourcingverträge geänderten technischen Gegebenheiten oder auch neuartigen Risiken angepasst werden müssen. Schon allein aufgrund der sich aus den Regeln zur Auftragsdatenverarbeitung ergebenden Anforderungen muss auch im Fall eines Outsourcings der jeweilige Auftraggeber stets über die aktuellen Sicherheitsmaßnahmen informiert sein. Aus datenschutzrechtlicher Sicht ist daher entscheidend, bei den Regeln zur laufenden Anpassung und Weiterentwicklung der Konzepte darauf zu achten, dass alle datenschutz- und sicherheitsrelevanten Änderungen stets einvernehmlich vorgenommen werden. Da die vorgelegten Entwürfe dieses noch nicht hinreichend deutlich erkennen ließen, baten wir um entsprechende Verdeutlichung. In dem bereits erwähnten Gespräch mit dem Innenministerium sagte dieses zu, dass der Grundsatz für alle Konzepte des Netzbetriebs mit datenschutzrelevantem Inhalt gelte, selbst für diejenigen, deren Inhalt das mit dem LVN-Betrieb beauftragte Unternehmen als Betriebsgeheimnis ansehe.

1.1.4 Transparente und klar voneinander abgegrenzte Zuständigkeitsbereiche

Um den Datenschutz bei der Verarbeitung personenbezogener Daten zu wahren, ist darauf zu achten, dass sich die konzipierten Maßnahmen auf alle Systeme erstrecken, die an der Datenverarbeitung beteiligt sind. Die vorgelegten Datenschutz- und Sicherheitskonzeptionen erstrecken sich auf etliche, aber nicht auf alle Aspekte, die sich bei der elektronischen Übertragung personenbezogener Daten über das Landesverwaltungsnetz und den Metronetzverbund ergeben. Da daran angeschlossene Stellen nach unserer Erfahrung darüber mitunter nicht ausreichend informiert sind, haben wir uns dafür ausgesprochen, Maßnahmen zu ergreifen, um die Transparenz gegenüber den nutzenden Stellen sowie den Auftraggebern zu erhöhen. Dabei muss diesen insbesondere deutlich gemacht werden, in welchen Bereichen sie weiterhin eigenständig Lösungen realisieren müssen. Das Innenministerium ließ uns mittlerweile wissen, dass es unser Anliegen teile, aber der Auffassung sei, dass bereits genug für die Information der nutzenden Stellen getan werde.

1.1.5 Regelmäßige Datenschutzrevisionen

Um eine Kontrolle der Einhaltung der Datenschutzanforderungen sicherzustellen, sollten von vornherein neben anlassbezogenen auch regelmäßige Überprüfungen vorgesehen werden. Neben Überprüfungen, die der Auftraggeber durchführen kann, kommen dabei auch Überprüfungen durch den Auftragnehmer in Betracht. Die dabei erzielten Ergebnisse sollten schriftlich festgehalten werden. Ferner sind die Auftraggeber über die Ergebnisse der Überprüfungen zu unterrichten. Wir haben angeregt, dass sich Auftraggeber und Auftragnehmer auf die regelmäßige Durchführung derartiger Datenschutzrevisionen verständigen. Das Innenministerium möchte dem jedoch nicht nachkommen. Es hält es für ausreichend, dass von Seiten der Auftraggeber jederzeit bei Bedarf eine solche Überprüfung der Auftragsabwicklung durchgeführt werden kann.

1.2 Netzwerksicherheit durch MPLS-Technik

Beim Aufbau und Betrieb von Telekommunikationsnetzen können Kosten seit einiger Zeit dadurch eingespart werden, dass die bisher zum Verbindungsaufbau erforderlichen aufwendigen Netzknotenrechner mit Hilfe von Geräten zur Kommunikation im Internet (Router) simuliert werden und die Kommunikation der einzelnen Benutzergruppen nur noch logisch voneinander getrennt wird. Die hierfür verwendete Technik nennt sich „multi protocol label switching“ (MPLS) und soll durch einen Zusatz an jedem Datenpaket einen sicheren Weg durch das Datennetz gewährleisten. Das Innenministerium und die mit dem Betrieb des Landesverwaltungsnetzes (LVN) beauftragte Stelle wollten sich die neue Technik zunutze machen und durch den Aufbau eines sog. Metronetzes als Teil des LVNs Kosten einsparen. Um die datenschutzrechtlichen Anforderungen beim Betrieb dieses Metronetzes einzuhalten, wurde das Datenschutz- und Sicherheitskonzept für das LVN fortgeschrieben und uns zur Prüfung vorgelegt.

Damit die Trennung der Datenströme, wie sie sich bei verbindungsorientierten Netzen bewährt hat, auch bei paketorientierten MPLS-Netzen funktioniert, sind eine Reihe von Maßnahmen zu treffen, die wir zwischenzeitlich dem Innenministerium vorgeschlagen haben. Im Kern geht es darum, die virtuellen Netze der einzelnen Benutzergruppen logisch sauber voneinander zu trennen und die Netzinfrastruktur vor Missbrauch zu schützen. Dies kann z. B. durch eine Trennung der Adressräume und Routinginformationen, durch eine „Unkenntlichmachung“ des Kernnetzes und seiner Komponenten gegenüber den Nutzern und durch eine besondere Absicherung der „Randbereiche“ und „Übergangsstellen“ der virtuellen Netze nach außen erfolgen.

Die Anforderungen an den Betrieb eines datenschutzrechtlich zulässigen und damit auch sicheren Netzwerks, über das getrennt zu haltende Datenströme verschiedenster Nutzer geleitet werden, sind hoch. Schon in der Zeit vor dem Outsourcing des Landesverwaltungsnetzes haben die beteiligten Stellen Erfahrungen in dieser Richtung sammeln können. Insofern bleibt auch für den Betrieb des Metronetzes zu hoffen, dass böse Überraschungen ausbleiben.

## 2. Datenschutz bei der Spam-Abwehr

Mittlerweile gehört es zu den leidvollen Erfahrungen vieler Computernutzer, mehr unverlangte E-Mail-Werbung und unerwünschte E-Mails zu erhalten als solche, die für sie tatsächlich von Interesse sind. Untersuchungen sprechen davon, dass derartige, vielfach auch als „Spam“ bezeichnete E-Mails in den letzten Monaten durchweg mehr als die Hälfte aller im Internet versandten E-Mails ausgemacht haben. Da auch Behörden und andere öffentliche Stellen des Landes davon nicht verschont bleiben, ist es nur zu verständlich, dass auch die Landesverwaltung nach Wegen sucht, um diese Problematik spürbar zu entschärfen. Bei der Planung von Spam-Abwehrmaßnahmen gilt es allerdings auch, den Datenschutz im Blick zu behalten, denn viele Maßnahmen zur Spam-Abwehr erfordern die Verarbeitung personenbezogener Daten. Ferner können derartige Maßnahmen unter Umständen auch einen ungerechtfertigten Eingriff in das Fernmeldegeheimnis darstellen.

Ein unzulässiger Eingriff in das Fernmeldegeheimnis kann beispielsweise dann vorliegen, wenn eine Dienststelle ihren Bediensteten die private Nutzung des E-Mail-Diensts gestattet hat und die Art der Verarbeitung personenbezogener Daten zur Spam-Abwehr nicht mit den zur privaten Nutzung berechtigten Personen abgestimmt worden ist. Ähnliche Konsequenzen kann es haben, wenn eine Schule, eine Hochschule oder eine öffentliche Bibliothek ihren Schülern, Studierenden oder Nutzern einen uneingeschränkten Internetzugang ermöglicht und personenbezogene Daten ohne vorherige Abstimmung mit ihnen zur Spam-Abwehr verarbeitet. Ein unzulässiger Eingriff in das Fernmeldegeheimnis kann ferner auch dann vorliegen, wenn eine Dienststelle den E-Mail-Dienst gegenüber Dritten, etwa Vereinen oder Firmen, anbietet und die für den Datenschutz und das Fernmeldegeheimnis relevanten Modalitäten der Spam-Filterung nicht mit die-

sen abgestimmt hat. Welche Probleme sich dabei in der Praxis ergeben können, ist z. B. auch der Beschreibung und der datenschutzrechtlichen Bewertung der von einer Universität vorgenommenen E-Mail-Filterung zu entnehmen, die wir in unserem 25. Tätigkeitsbericht (LT-Drucksache 13/3800) sowie in unserem 26. Tätigkeitsbericht (LT-Drucksache 13/4910) angesprochen haben.

Eine vom Innenministerium geplante Vorgehensweise zur Spam-Abwehr trug den datenschutzrechtlichen Anforderungen noch nicht ausreichend Rechnung. Zur Begründung der von ihm vorgeschlagenen Anti-Spam-Maßnahmen verwies es auf folgenden Zusammenhang: Viele an die Landesverwaltung gerichtete Spam-Mails waren nicht an tatsächlich existierende E-Mail-Adressen gerichtet, sondern an Adressen der Form Vorname.Nachname@Dienststelle.bwl.de, bei denen zwar eine zutreffende Dienststellenbezeichnung genannt wurde, die verwendeten Vor- und Nachnamen aber frei erfunden worden waren. Derartige E-Mails konnten an kein E-Mail-Postfach zugestellt werden. Dies wiederum hatte zur Folge, dass dementsprechend auch eine Vielzahl von Unzustellbarkeitsnachrichten durch die E-Mail-Server des Landes versandt wurden. Da vielfach aber auch die Absender-Adressen der Spam-Mails frei erfunden waren, konnten auch etliche Unzustellbarkeitsnachrichten nicht zugestellt werden. Mehr noch: Dies führte dazu, dass E-Mail-Server des Landes in einigen Spam-Filterlisten als Spam-Quellen genannt wurden mit der Folge, dass zwischen der Landesverwaltung und anderen Stellen, die sich auf diese Spam-Filterlisten verließen, keine Kommunikation mehr möglich war. Um diese, wenn auch nur mittelbar durch Spam verursachten Kommunikationsstörungen zu vermeiden, schlug das Innenministerium vor, dass das Land seinerseits Spam-Filterlisten (sog. Blacklists) verwenden solle, in denen jeweils Einrichtungen, Absender oder E-Mail-Server genannt sind, von denen erfahrungsgemäß Spam-Nachrichten ausgehen.

Uns erschien dies so, als wolle das Innenministerium den Teufel mit dem Beelzebub austreiben. Denn wir hielten es zumindest für zweifelhaft, ob gerade die eigene Anwendung von Blacklists diejenigen Probleme lösen kann, die gerade durch eine von anderen Stellen vorgenommene Blacklist-basierte Spam-Filterung hervorgerufen wurden. Zumindest wenn man sich dabei, wie dies häufig geschieht, ohne weitere Prüfung auf die Qualität der von Dritten gepflegten Blacklists verlässt, ist damit zu rechnen, dass darin seriöse Kommunikationspartner ebenso auftreten können, wie Systeme der Landesverwaltung selbst auf einigen derartigen Listen auftraten. Dass das Innenministerium die Verwendung der Blacklists derart in den Mittelpunkt seiner Anti-Spam-Strategie rückte, überraschte uns umso mehr, als das Landesrechenzentrum, das die zentralen E-Mail-Server betreibt, bereits vor Jahren darauf hingewiesen hat, dass auf Blacklists ein „erheblicher Anteil“ an „Unschuldigen“ geführt werde, die bei deren Anwendung zu Unrecht von der Kommunikation ausgeschlossen werden.

Aus Sicht des Datenschutzes ist für die Spam-Abwehr von Bedeutung, dass dafür eine Vielzahl an Maßnahmen herangezogen werden kann. Einen Eindruck hierüber vermittelt u. a. die Anti-Spam-Studie des Bundesamts für Sicherheit in der Informationstechnik *(http://www.bsi.de/literat/studien/antispam/index.htm)*. Die einzelnen Maßnahmen sowie denkbare Kombinationen dieser Maßnahmen unterscheiden sich u. a. auch hinsichtlich des Ausmaßes, in dem dabei in die Persönlichkeitsrechte der Kommunikationspartner sowie Dritter eingegriffen wird, deren personenbezogenen Daten in den verarbeiteten E-Mails enthalten sein können. Ziel einer datenschutzgerechten Anti-Spam-Strategie muss es daher sein, nach einer Lösung zu suchen, bei der möglichst wenige personenbezogene Daten verarbeitet werden und möglichst wenig in die Persönlichkeitsrechte der Kommunikationspartner und anderer Betroffener eingegriffen werden muss.

Der Konzeption des Innenministeriums, die allein auf Blacklists setzte, war nicht zu entnehmen, dass eine solche Abwägung der in Betracht kommenden Maßnahmen vorgenommen worden war. Gerade da unzulänglich konzipierte Anti-Spam-Maßnahmen mehr schaden als nutzen können, forderten wir das Innenministerium zu einer entsprechenden Überarbeitung seiner Anti-Spam-Strategie auf.

Um zu vermeiden, dass eine unzureichend konzipierte Anti-Spam-Maßnahme Verletzungen der Persönlichkeitsrechte der Betroffenen oder des Fernmeldegeheimnisses nach sich zieht, sollten bei der Erstellung einer Anti-Spam-Strategie u. a. folgende Hinweise beachtet werden:

– Eine in der Regel schriftlich auszuarbeitende Anti-Spam-Strategie muss erkennen lassen, dass unter den in Betracht kommenden Maßnahmen diejenigen ausgewählt wurden, die mit den geringsten Eingriffen in die Persönlichkeitsrechte der Betroffenen verbunden sind.

– Ferner sollten insbesondere solche Maßnahmen in Betracht gezogen werden, die außerhalb der Reichweite des Fernmeldegeheimnisses eingreifen.

– Nicht zuletzt sollten die Empfänger der Nachrichten in größtmöglicher Autonomie über den Umgang mit den an sie gerichteten E-Mails selbst entscheiden können. Moderne E-Mail-Programme bieten den Nutzern dazu eine Reihe von Möglichkeiten, um die eingehende Post nach bestimmten Kriterien zu sortieren und dementsprechend z. B. in unterschiedlichen Postfächern abzulegen. Zum Teil lassen sich diese Programme bis zu einem gewissem Grad zur Spam-Erkennung „trainieren“. Der Nutzer muss dazu zunächst für eine Reihe von E-Mail-Sendungen, die er erhält, angeben, ob er diese als Spam bewertet oder nicht. Ein Vorteil dieses „Trainings“ ist, dass sich die Filterung an den Vorstellungen und Bewertungsmaßstäben des trainierenden Nutzers orientiert.

– Viele Spam-Definitionen umfassen ein subjektives Element. Dies zeigt sich etwa, wenn man Spam als „unerwünschte E-Mail“ oder „unerwünschte Werbe-E-Mail“ definiert, darin, dass von Nutzer zu Nutzer ganz unterschiedliche Auffassungen darüber bestehen können, was diese jeweils als unerwünscht ansehen. Schon allein aus diesem Grund können Anti-Spam-Maßnahmen in der Regel keine absolut zuverlässige Spam-Erkennung bieten. Anti-Spam-Maßnahmen, die zu einer Markierung einer empfangenen E-Mail führen, sind daher solchen Maßnahmen vorzuziehen, bei denen E-Mails automatisch gelöscht werden.

### 3. Unzureichender Zugriffsschutz im lokalen Netz eines Landratsamts

Wie schon in früheren Jahren mussten wir bei einem Kontrollbesuch auch in diesem Jahr wieder gravierende Unzulänglichkeiten beim Betrieb eines lokalen Computernetzwerks (LAN) feststellen. Die Folge war, dass zahlreiche Nutzer eines Landratsamts auf personenbezogene Daten zugreifen konnten, die sie zur Erledigung ihrer dienstlichen Aufgaben überhaupt nicht benötigten. Unter anderem konnten Bedienstete des Gesundheitsamts auf ca. 15 000 Abfallgebührenbescheide aus dem laufenden Jahr zugreifen. Diesen Bescheiden waren u. a. jeweils Namen und Anschrift des Rechnungsempfängers, das Buchungszeichen, die Anschrift des Objekts, für das die Gebühr erhoben wird, die Anzahl, Größe und der Leerungsrhythmus der in Rechnung gestellten Abfallbehälter (z. B. „Biomüllbehälter 120 l 2-wöchentlich“ oder „Windeltonne 120 l 2-wöchentlich“), der Zeitraum, für den die Gebühren jeweils erhoben werden, sowie die Jahresgebühr zu entnehmen. Ferner ließen sich den Bescheiden auch die Fälligkeitsdaten der Rechnungsbeträge sowie Angaben darüber entnehmen, ob das jeweilige Gebührenkonto vor dieser Veranlagung ausgeglichen war. Schließlich enthielten die Bescheide den Hinweis darauf, dass die Gebühren von einem jeweils durch Kontonummer und Bankleitzahl bezeichneten Konto abgebucht werden.

Daneben konnte vom Gesundheitsamt aus auch auf Daten aus dem Zeiterfassungssystem sowie aus anderen Anwendungen zugegriffen werden, die nicht für die Nutzung durch das Gesundheitsamt bestimmt waren. Obwohl an dem überprüften Arbeitsplatz die zur Nutzung dieser Anwendungen bestimmte Software nicht installiert war, war es vielfach mit Hilfe eines einfachen Textverarbeitungsprogramms gleichwohl möglich, die in diesen Anwendungen erfassten Daten, darunter auch personenbezogene Daten, zumindest teilweise zu lesen oder sogar zu ändern. So waren u. a. Uhrzeitangaben und Namen lesbar, die vom Zeiterfassungssystem für die Beschäftigten des Landratsamts gespeichert wurden.

Die Zugriffsberechtigungen waren dabei vielfach so gestaltet, dass nicht nur Bedienstete des Gesundheitsamts, sondern alle Mitarbeiterinnen und Mitar-

beiter des Landratsamts, die einen PC nutzen, die genannten Dokumente hätten öffnen, lesen und auch ändern können, und zwar unabhängig davon, ob sie diese Daten zur Erledigung ihrer dienstlichen Aufgaben benötigten oder nicht.

Besonders kritisch daran war, dass der unberechtigte Zugriff gleich auf Daten einer Vielzahl von Personen möglich war. Als kritisch war zudem zu bewerten, dass sich Dateien, die von Fachverfahren (wie z. B. dem Zeiterfassungssystem) verarbeitete Daten enthielten, lesen oder sogar ändern ließen, ohne zuvor das entsprechende Fachverfahren starten zu müssen. Die Zugriffskontrolle der entsprechenden Fachverfahren hätte sich auf diese Weise umgehen lassen und war dadurch deutlich geschwächt.

Alles in allem lag damit ein schwerwiegender Mangel der Zugriffs- und Organisationskontrolle vor, den ich beanstandet habe. Ich forderte das Landratsamt auf, so bald wie möglich Konzeptionen für die Gewährung der Zugriffsmöglichkeiten für die Dateiablage zu erarbeiten und sicherzustellen, dass nicht zulässige Zugriffe technisch auch nicht mehr durchgeführt werden können. Daneben waren im Rahmen des vom Landratsamt zu erstellenden Datenschutz- und Sicherheitskonzepts für den Betrieb des lokalen Netzwerks Ablagekonzepte zu erarbeiten und umzusetzen, die verhindern, dass Nutzer durch Direktzugriff auf die von den Fachverfahren benutzten Dateien an Daten gelangen können, die nicht für sie bestimmt sind. Vorgaben zur Konfiguration der einzelnen Arbeitsplatz-PCs waren dazu ebenso erforderlich wie Richtlinien darüber, wer unter welchen Voraussetzungen Daten für einen Zugriff über Netz freigeben darf.

Zu begrüßen ist, dass das Landratsamt aus den Feststellungen beim Kontrollbesuch Konsequenzen gezogen und umgehend die „Neuregelung und Dokumentation der Zugriffsberechtigungen auf die Dateiablage“ in Aussicht gestellt hat.

**4. Fernzugriff auf Dateien durch untere Verwaltungsbehörden**

Schon seit einiger Zeit nutzen die unteren Verwaltungsbehörden, z. B. die Landratsämter, EDV-Verfahren des Landes, die von einem Zentralrechner des Landes zur Verfügung gestellt werden. Durch die Eingliederung zahlreicher Sonderbehörden im Zuge der Verwaltungsreform hat sich dieser Trend noch verstärkt. Technisch läuft die Sache dabei häufig so ab, dass der Arbeitsplatzrechner im Landratsamt als Terminal (Client) des Zentralrechners (Server) fungiert und von dort aus auf im Zentralrechner hinterlegte personenbezogene Daten des jeweiligen Fachverfahrens zugegriffen wird. Bei einem Fachverfahren zur Lebensmittelüberwachung (LÜVIS) im Geschäftsbereich des Ministeriums für Ernährung und Ländlichen Raum, das uns um Rat gefragt hatte, haben wir festgestellt, dass sich dabei unter Umständen empfindliche Sicherheitslücken auftun können. Bei Verwendung eines bestimmten Terminalprogramms ist es nämlich möglich, vom Zentralrechner des Landes aus – also quasi aus der Ferne – auf den Arbeitsplatzrechner und gegebenenfalls auf hiermit verbundene Server beim Landratsamt zuzugreifen.

Dies wäre vielleicht nicht weiter schlimm, wenn dort nur das besagte Fachverfahren abliefe. Nun laufen jedoch auf den Arbeitsplatzrechnern der unteren Verwaltungsbehörden und erst recht auf dort eingesetzten Servern eine Reihe von anderen Fachverfahren ab, die mit dem Fachverfahren des Ministeriums nichts zu tun haben; ebenso sind auf den Festplatten dieser Rechner in der Regel zahlreiche personenbezogene Daten gespeichert, die das Ministerium bzw. den Zentralrechner des LÜVIS-Verfahrens nichts angehen. Da die Anwender in den unteren Verwaltungsbehörden die Daten des Fachverfahrens in einem Textverarbeitungsprogramm weiter verarbeiten müssen, mussten sie sich bisher die jeweilige Datei an die eigene E-Mail-Adresse schicken, was natürlich Verfahrensverzögerungen mit sich brachte. Durch die neue Version des Terminalprogramms sollte der Terminalserver einen schreibenden und lesenden Zugriff auf die lokalen Laufwerke des Arbeitsplatzrechners (Client) erhalten, damit dort die weitere Bearbeitung nahtlos fortgesetzt werden kann. Allerdings hat unsere Untersuchung ergeben, dass die Sache einen Haken hat: Clientseitig ist nämlich nicht kontrollierbar, auf welche Client-Laufwerke der Terminalserver wie zugreifen kann. Alle Cli-

ent-Laufwerke – auch solche, die über das lokale Netzwerk der unteren Verwaltungsbehörde eingebunden werden – stellt der Client-PC dem Terminalserver für beliebige Zugriffe zur Verfügung. Es war nicht ersichtlich, wie der Zugriff clientseitig durch eine entsprechende Berechtigungsvergabe beschränkt werden kann. Diese offenen Punkte müssen rasch geklärt werden, weil sich hier ein generelles Problem abzeichnet, das weniger mit dem konkreten Fachverfahren des Ministeriums für Ernährung und Ländlichen Raum als vielmehr mit dem – möglicherweise auch bei anderen Fachanwendungen eingesetzten – Terminalprogramm zu tun hat.

Generell halten wir es für erforderlich, dass bei einem Dateizugriff aus der Ferne sowohl auf der speichernden als auch auf der abrufenden Seite Maßnahmen ergriffen werden können, die unberechtigte Zugriffe unterbinden. Der Zugriff sollte zumindest durch Maßnahmen zur Authentisierung und Authentifizierung abgesichert werden. Dabei sollten die Zugriffsmethoden Maßnahmen zur Autorisierung mit der erforderlichen Differenzierung unterstützen. Bei entsprechender Anforderung sollten zusätzliche Maßnahmen zur Gewährleistung der Vertraulichkeit der Datenübertragung ergriffen werden.

Zur Realisierung dieser Anforderungen bieten sich mehrere technische Alternativen an, die wir dem Ministerium für Ernährung und Ländlichen Raum mitgeteilt haben. Wir können uns durchaus vorstellen, dass der Zugriff auf Client-Laufwerke datenschutzrechtlich unbedenklich gelöst werden kann, wenn – und das ist wesentlich – unter der Zugriffskontrolle des Betriebssystems des Clients wirksam geregelt werden kann, auf welche Client-Laufwerke vom Terminalserver wie zugegriffen wird. Letztlich ist die jeweilige untere Verwaltungsbehörde aber die für den Datenschutz im eigenen Bereich verantwortliche Stelle; sie muss wissen, ob sie sich auf das Risiko eines unkontrollierten Zugriffs auf ihre Datenbestände aus der Ferne einlassen will.

### 5. Clearingstelle für das Meldewesen

Wer seinen Wohnsitz ändert, musste sich bisher bei der alten Meldebehörde abmelden und bei der Meldebehörde des neuen Wohnsitzes anmelden. Zukünftig entfällt die Abmeldung, denn die für den neuen Wohnsitz zuständige Meldebehörde teilt die Abmeldung der alten Meldebehörde in einer sog. Rückmeldung mit. Diese Rückmeldung umfasst nicht nur den Umzug selbst, sondern eine Reihe von personenbezogenen Daten wie beispielsweise gegenwärtige, frühere und künftige Anschriften, Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die letzte frühere Anschrift im Inland oder Angaben zum gesetzlichen Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Sterbetag!). Aber damit nicht genug: Die Rückmeldung soll, statt wie bisher postalisch, in einem elektronischen Verfahren erfolgen. Zwar dürfte das für die Meldeämter keine unüberwindbaren Hürden darstellen, wenn der Umzug innerhalb Baden-Württembergs erfolgt. Die überwiegende Mehrzahl der Kommunen lässt ihre Meldedaten von zwei kommunalen Rechenzentren verarbeiten, die zudem über ein Netzwerk verbunden sind. Die Realisierung der elektronischen Rückmeldung sollte in diesem Fall mit überschaubarem Aufwand erledigt werden können.

Eine ganz andere Sachlage ergibt sich, wenn ein Bürger von einem anderen Bundesland nach Baden-Württemberg zieht oder ein Bürger aus Baden-Württemberg in ein anderes Bundesland. Immerhin gibt es bundesweit ca. 5 400 Meldebehörden. Weiter verkompliziert wird die Sache dadurch, dass nicht nur die Meldebehörde des früheren Wohnorts, sondern auch die Meldebehörden, bei denen der Betroffene mit einer Nebenwohnung gemeldet ist, eine Rückmeldung erhalten müssen. Die zuständigen Meldeämter auszumachen, ist dann nicht ganz einfach.

Damit die Rückmeldung tatsächlich bei der früheren Meldebehörde ankommt und nicht jede Meldebehörde mit großem Aufwand die elektronischen Erreichbarkeitsdaten von ca. 5 400 Meldeämtern aktuell halten und ihre eigene Erreichbarkeit für 5 400 Meldebehörden gewährleisten muss, hat man sich auf Bundes- und Länderebene hinsichtlich der Ländergrenzen überschreitenden Umzüge auf die Schaffung von sog. Clearingstellen ge-

einigt. Der Vorgang der Rückmeldung stellt sich dann etwa so dar: Die Rückmeldung wird von der Meldebehörde des neuen Wohnsitzes an die Clearingstelle ihres Bundeslands geschickt, diese schickt die Rückmeldung an die Clearingstelle des Bundeslands, in dem der Betroffene seinen alten Wohnsitz hatte. Von dort wird die Rückmeldung an die frühere Meldebehörde weiter vermittelt. Für die Übertragung der Daten wurde mit XMeld eine von allen Beteiligten einzuhaltende Datenbeschreibung geschaffen und für den Datentransport das Protokoll OSCI festgelegt, das die Signatur, Verschlüsselung und Quittierung der Zustellung der Rückmeldung ermöglicht.

Dass bei der Rückmeldung personenbezogene Daten verarbeitet werden, ist angesichts der oben beispielhaft erwähnten Daten unschwer zu erkennen. Wenn eine eigens dafür gebildete Clearingstelle die Übermittlung personenbezogener Daten durchführt, handelt es sich um eine Verarbeitung personenbezogener Daten im Auftrag nach § 7 LDSG. Das hat auch das mit der Realisierung der Clearingstelle beauftragte Rechenzentrum erkannt und uns gebeten, bei der Beantwortung der Frage mitzuwirken, wie seine Beauftragung durch die Kommunen vonstattenzugehen habe. Den Inhalt des bisher geltenden Vertrags über die Verarbeitung von Meldedaten durch das Rechenzentrum gemäß § 7 LDSG hat es uns zur Kenntnis gegeben.

Wir haben dem Rechenzentrum geantwortet, dass wir in der Erweiterung des bisher schon praktizierten Verfahrens um die Funktionalität der elektronischen Rückmeldung eine bloße Verfahrensänderung sehen. Ein neues Verfahren liegt unserer Meinung nach jedoch nicht vor. Daher bedarf es auch keiner erneuten Beauftragung durch die Kommunen. Da das Rechenzentrum Auftragnehmer für die Durchführung des Meldeverfahrens und der Clearingstelle ist, ergibt sich aus dem Vertrag die datenschutzrechtliche Zulässigkeit der Vornahme von Rückmeldungen durch das Rechenzentrum.

Ein anderes Ergebnis könnte sich im Fall des zweiten Rechenzentrums ergeben. Wenn dieses die vom ersten Rechenzentrum betriebene Clearingstelle für die bundesweite Rückmeldung nutzt, dann lässt es personenbezogene Daten in einem Unterauftragsverhältnis verarbeiten. Diese Möglichkeit sieht das Landesdatenschutzgesetz in § 7 ausdrücklich vor. Allerdings müsste sich das Rechenzentrum im Vertrag über die Verarbeitung personenbezogener Daten mit seinen Kommunen das Recht auf Einschaltung Dritter im Unterauftragsverhältnis nach § 7 LDSG ausbedungen haben. Wenn das der Fall ist, wäre die Nutzung der Clearingstelle durch das Rechenzentrum datenschutzrechtlich zulässig. Sollte das Rechenzentrum allerdings für die ihm übertragene Datenverarbeitung keine Unterauftragsverhältnisse eingehen dürfen, dann müssten die an das Rechenzentrum angeschlossenen Kommunen ihm durch Erweiterung des Vertrags oder der Clearingstelle in einem neuen Vertrag den Auftrag zur Vornahme der Rückmeldungen erteilen.

### 6. Das „Elektronische Gewerberegister“

Wie alle Dinge auf Erden unterliegt auch Software der Alterung. Sei es, dass die Softwaresysteme auf neuen Rechnersystemen nicht mehr ablaufen oder dass der technische Fortschritt bei den Benutzerschnittstellen und -oberflächen die Programme „alt“ aussehen lässt. So geschehen ist es mit einem Programm für die Verwaltung der Gewerberegister der Kommunen des DV-Verbunds Baden-Württemberg. Deshalb wurde ein neues Programm entwickelt und in zwei Kommunen in Piloteinsatz gebracht. Bei einer der Kommunen führten meine Mitarbeiter einen Kontrollbesuch durch, um sich schon im Frühstadium über die datenschutzrechtlich zulässige Verarbeitung personenbezogener Daten zu vergewissern und gegebenenfalls auf Änderung zu drängen.

Neben der Kontrolle des Verfahrens, das heißt der Prüfung, welche Daten gespeichert werden können und wie die Daten verarbeitet werden, ist regelmäßiger Prüfpunkt, wann, von wem und wie personenbezogene Daten gelöscht werden. Hierbei gibt es unterschiedlichste Ausprägungen. Die Bandbreite reicht von löschfristgerechten taggenauen automatischen Löschläufen bis zur – und das ist mit Hinblick auf den Datenschutz die schlechteste Lösung – manuellen Löschung durch die Mitarbeiter ohne programmseitige Benachrichtigung über die zu löschenden Daten. Dass man

bei letzterer Vorgehensweise auch mal das eine oder andere zu löschende Datum übersieht, ist bei der Menge an mittlerweile zu verarbeitenden Daten nahezu zwangsläufig.

In der Praxis sieht es leider oft noch betrüblicher aus, wie meine Mitarbeiter beim Kontrollbesuch einer württembergischen Großen Kreisstadt entdecken mussten:

Die Kommune hatte die Chance für einen Neuanfang ungenutzt verstreichen lassen und die Datensätze vom alten Verfahren ohne Vorverarbeitung, die im Falle der Inbetriebnahme eines neuen Softwaresystems mit Altdaten eigentlich immer durchgeführt werden muss, in das neue Verfahren übernommen. Bei der stichprobenweisen Sichtung der Datenbestände des neuen Verfahrens wurden meine Mitarbeiter in mehrfach bedenklicher Weise fündig. Wir stießen im „Elektronischen Gewerberegister“ zum Beispiel auf Gewerbe, die in den Jahren 1971, 1983, 1993 beziehungsweise 1994 abgemeldet worden waren. Dies weist auf Folgendes hin:

– Obwohl die Stadt für die Löschung in ihrem Verfahrensverzeichnis eine Löschfrist angegeben hat – wobei deren Dauer von zehn Jahren nicht ohne weiteres nachzuvollziehen ist –, ist auch nach Ablauf dieser Zeit die Löschung nicht vorgenommen worden.

– Die (Gewerbeanzeigen-)Datenbestände der Stadt wurden bei der Migration aus dem früheren Verfahren in das „Elektronische Gewerberegister“ in dieses Verfahren auch dann übernommen, wenn sie bereits zu löschen gewesen wären.

– Auch beim Betrieb des Vorgängerverfahrens war die Löschung der Daten nicht vorgenommen worden.

Was die Löschung personenbezogener Daten betrifft, werden bzw. wurden demnach sowohl das aktuelle Verfahren als auch (das) Vorgängerverfahren nicht datenschutzgerecht betrieben. Wir forderten daher die Stadt auf, Daten, bei denen die Voraussetzungen der Löschung bereits vorliegen, umgehend zu löschen, und uns auch über die Maßnahmen zu unterrichten, die die Stadt ergreift, um zukünftig die fristgerechte Löschung der Daten zu gewährleisten. Die Stadt begründete die äußerst ungenügende Löschpraxis damit, dass bisweilen Gewerbetreibende um einen Nachweis zur Durchsetzung verschiedenster Ansprüche wie beispielsweise gegenüber der Rentenversicherung nachfragten. Hierzu ist Folgendes zu sagen:

– Jeder Gewerbetreibende ist selbst dafür verantwortlich, dass er seine Unterlagen, die den Gewerbebetrieb nachweisen, über die erforderliche Zeitdauer aufbewahrt.

– Die Zweckbindung der im Gewerberegister gespeicherten Daten besteht in der Überwachung des Gewerbebetriebs. Wenn ein Gewerbe eröffnet wird, gehen in der Regel Meldungen hierüber an eine Vielzahl von Behörden (Eichamt, Lebensmittelkontrolle, Finanzamt, etc.), worauf diese Behörden ihrerseits die erforderlichen Maßnahmen ergreifen. Die Erfassung der Meldung eines Gewerbebetriebs an einer Stelle und die sich daraus ergebende Verwaltungsvereinfachung ist ein zentraler Gedanke des Gewerberegisters. Der Nachweis des Gewerbebetriebs gegenüber dem Gewerbetreibenden gehört nicht zu diesen Aufgaben.

– Wenn die Kommune Daten im Interesse der Betroffenen länger speichern möchte, als es der Kommune vorgeschrieben oder zur Erfüllung ihrer Aufgaben erforderlich ist, sollte sie das nur tun, wenn die Betroffenen das wünschen und ihre Einwilligung dazu erklärt haben.

### 7. Hackers Traum – Bankverbindungen im Internet abrufbar

Bisweilen sind die datenschutzrechtlichen Verstöße so schwerwiegend, dass ein sofortiges Einschreiten meinerseits erforderlich ist. Einen in dieser Hinsicht besonderen Fall musste ich im Oktober 2006 feststellen. Und das kam so:

Beschäftigte der Landesverwaltung können seit einiger Zeit ein sog. Job-Ticket der Deutschen Bahn AG für die Fahrt vom Wohnort zum Arbeitsplatz erwerben; ein vergleichbares Angebot gibt es auch für den Nahverkehr

des VVS-Verbunds in der Region Stuttgart. Damit sichergestellt ist, dass nur Berechtigte ein Job-Ticket erwerben können, will das (jeweilige) Beförderungsunternehmen nachprüfen, ob die Besteller wirklich für die Landesverwaltung tätig sind. Dazu haben sich das Landesamt für Besoldung und Versorgung und das bzw. die Beförderungsunternehmen ein internetgestütztes Bestellverfahren ausgedacht. Die Beschäftigten der Landesverwaltung melden sich über das Internet beim sog. Kundenportal des Landesamts mit Personalnummer und Kennwort an. Dort müssen sie in einem Dialog eine E-Mail-Adresse und Telefon-Nummer angeben, unter der sie erreichbar sind, und die Richtigkeit der schon beim Landesamt gespeicherten Angaben zu Wohnort, Geburtsdatum und Bankverbindung – bestehend aus Bankleitzahl, Kontonummer und Name des Kontoinhabers – überprüfen und gegebenenfalls korrigieren. Durch Drücken eines entsprechenden graphischen Bedienelements („Button“) wird dann ein weiteres Fenster geöffnet und die Benutzer gelangen entweder zu einem Bestellformular für eine Jahreskarte (der Deutschen Bahn AG) oder zu einem Formular für die Bestellung einer VVS-Jahreswertmarke. In diesem Fenster werden diese Angaben nochmals aufgeführt und können geändert oder bestätigt werden, bevor man durch Drücken eines „Weiter“-Buttons zu einem Formular gelangt, auf dem die gewünschte Verkehrsverbindung oder die Verbundpassnummer des VVS-Ausweises eingegeben werden muss. Nach einer rechtlichen Belehrung erscheint eine Seite, auf der alle Angaben nochmals aufgeführt werden. Durch Drücken des „Bestellen“-Buttons wird eine Bestellung durchgeführt und auf einer weiteren Internet-Seite mitgeteilt, dass die Bestellung entgegengenommen wurde und dass demnächst eine Auftragsbestätigung per E-Mail an die angegebene E-Mail-Adresse erfolgen wird. Zudem besteht auf dieser Seite die Möglichkeit, über einen in den Text eingebauten WWW-Verweis die Auftragsbestätigung als sog. pdf-Dokument abzurufen und auszudrucken. Und genau hier hatte das Verfahren eine erhebliche Sicherheitslücke, konnte doch durch Verändern eines Teils dieses Verweises auf Auftragsbestätigungen von anderen Beschäftigten der Landesverwaltung zugegriffen werden.

In einem Telefax, das Ende Oktober bei der Dienststelle einging, machte uns ein Beschäftigter der Landesverwaltung darauf aufmerksam, dass bei Kenntnis der Zusammensetzung des Verweises jeder über das Internet Auftragsbestätigungen abrufen kann. Meine Mitarbeiter machten sich sofort daran, den Sachverhalt zu überprüfen. Und tatsächlich: Schon der Abruf des WWW-Verweises der eigenen Bestellung in einem neuen Zugriff nach Abschluss des Bestelldialogs funktionierte anstandslos, obwohl man erwarten würde, dass der Verweis nur für den Bestelldialog gültig ist und danach ins Leere führt. Durch Verändern von zwei Angaben, wobei eine die laufende Nummer des Auftragseingangs war, konnten meine Mitarbeiter eine Reihe von Auftragsbestätigungen abrufen. Wir gehen aufgrund unserer Stichprobe davon aus, dass personenbezogene Daten wie Name, Vorname, Wohnort, Straße und Hausnummer, E-Mail-Adresse, Bankleitzahl, Kontonummer, Name des Kontoinhabers und Name des Kreditinstituts sowie die Strecke und Klasse der Bahnverbindung, die mit der Jahreskarte bereist werden kann, von ca. 9 000 Beschäftigten der Landesverwaltung im Internet abrufbar waren. Mit ein wenig Programmieraufwand hätten alle pdf-Dokumente automatisch abgerufen, die personenbezogenen Daten aus den pdf-Dokumenten extrahiert und beliebig weiterverarbeitet werden können. Ein böswilliger Angreifer hätte die Sicherheitslücke möglicherweise zu noch weiter reichenden Offenbarungen personenbezogener Daten ausnutzen können, wenn es ihm gelungen wäre, durch die Sicherheitslücke hindurch eigene Datenbankanfragen an die Datenbank zu stellen.

Wenn derart sensible personenbezogene Daten von jedermann über das Internet abrufbar sind, ist sofortiges Handeln oberstes Gebot. Per Telefax – das Landesamt für Besoldung und Versorgung eröffnet leider nicht die Möglichkeit, ihm verschlüsselte E-Mail-Nachrichten zukommen zu lassen – habe ich die Behörde auf die Sicherheitslücke hingewiesen und gebeten, mir kurzfristig mitzuteilen, was dagegen veranlasst wird. Immerhin übermittelt das Landesamt die personenbezogenen Daten an Dritte, wobei es nicht davon ausgehen kann, dass die Beschäftigten mit Wissen darüber, dass ihre Bankverbindung von jedermann über das Internet abgerufen wer-

den kann, der Übermittlung zugestimmt hätten. Dass das Landesamt mit der Sache etwas zu tun hat, müssen die Besteller schon deshalb annehmen, weil auf jeder Internet-Seite des Bestelldialogs sein Briefkopf eingeblendet wird.

Noch am Nachmittag des Tages, an dem wir uns an das Landesamt gewandt hatten, stellten wir fest, dass der Zugriff auf die Auftragsbestätigungen mit Hinweis auf dringend durchzuführende Wartungsarbeiten unterbunden war. Das Landesamt teilte mir dann in einer Voraberklärung mit, dass es die Übermittlung der Daten unverzüglich unterbunden hat. Die Sicherheitslücke sei auf einen Mangel beim Zusammenwirken von zwei Servern des Beförderungsunternehmens zurückzuführen. Das vom Beförderungsunternehmen mit der Erstellung der Software beauftragte Unternehmen arbeite an der Beseitigung der Sicherheitslücke. Eine abschließende, detaillierte Stellungnahme steht noch aus. Hoffentlich widmen sich die Verantwortlichen der notwendigen datenschutzgerechten Lösung genauso hingebungsvoll, wie sie die Abbuchung des Ticketpreises organisiert hatten: Zur Verärgerung vieler Landesmitarbeiter war das Ticketentgelt nämlich schon von ihren Konten abgebucht, bevor sie das Ticket überhaupt in Händen hatten und lange vor dem Geltungsbeginn der Jahreswertmarke.

## Inhaltsverzeichnis des Anhangs

Anhang 1

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 26./27. Oktober 2006**

**Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten**

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz – BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat – sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem – in einigen Landesverfassungen ausdrücklich genannten – Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

– Die Antiterrordatei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

– Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtiger führen.

– Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z. B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

– In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

– Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfeld-

daten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

– Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Anhang 2

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 26./27. Oktober 2006**

**Das Gewicht der Freiheit beim Kampf gegen den Terrorismus**

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der „Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes“ kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes“ ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anhang 3

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 16./17. März 2006**

**Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen**

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat*. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u. a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtige, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt – einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

---

* KOM (2005) 475 vom 4. Oktober 2005

Anhang 4

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 16./17. März 2006**

**Listen der Vereinten Nationen und der Europäischen Union**
**über Terrorverdächtige**

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z. B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwerwiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Anhang 5

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 16./17. März 2006**

**Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht**

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über – durch das Fernmeldegeheimnis geschützte – Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses – erstmals zur Durchsetzung wirtschaftlicher Interessen – zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Anhang 6

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 26./27. Oktober 2006**

**Keine Schülerstatistik ohne Datenschutz**

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte „Schulleben" ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen „Bildungsregisters" nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

Anhang 7

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 16./17. März 2006**

**Keine kontrollfreien Räume bei der Leistung von ALG II**

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Anhang 8

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 15. Dezember 2005**

**Sicherheit bei eGovernment durch Nutzung des Standards OSCI**

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von so genannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Kooperationsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Anhang 9

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 26./27. Oktober 2006**

**Verbindliche Regelungen für den Einsatz von RFID-Technologien**

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

– Transparenz

  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

– Kennzeichnungspflicht

  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

– Keine heimliche Profilbildung

  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine

Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

– Vermeidung der unbefugten Kenntnisnahme

  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

– Deaktivierung

  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anhang 10

**Entschließung**
**der Datenschutzbeauftragten des Bundes und der Länder**
**vom 11. Oktober 2006**

(bei Enthaltung von Schleswig-Holstein)

**Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren**

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfs der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87 a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicherweise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

– Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,

– immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,

– die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anhang 11

**Bekenntnis**
**zur freiheitlichen demokratischen Grundordnung**
**nach dem Staatsangehörigkeitsgesetz (StAG)**

**Gesprächsleitfaden für die Einbürgerungsbehörden**
**Stand 1. September 2005**

Name, Vorname und ggf. Geburtsname des Einbürgerungsbewerbers:

Geburtsdatum: Nationalität:

Vorbemerkung:

Das Bekenntnis zur freiheitlichen demokratischen Grundordnung des Grundgesetzes für die Bundesrepublik Deutschland ist Einbürgerungsvoraussetzung nach § 10 Abs. 1 Satz 1 Nr. 1 StAG. Entsprechendes gilt im Rahmen der Ermessenseinbürgerung. Es darf deshalb keineswegs als Formalie gehandhabt werden, die mit der Unterschrift unter die Bekenntniserklärung erfüllt ist. Soweit die Einbürgerungsbehörde Zweifel hat, ob der Einbürgerungsbewerber den Inhalt seiner Erklärung wirklich verstanden hat und ob sie seiner inneren Überzeugung entspricht, führt sie ein Gespräch mit ihm unter Verwendung dieses Leitfadens. Die Ergebnisse des Gesprächs sind zu dokumentieren und vom Einbürgerungsbewerber zu unterschreiben. Dabei sind auch Erläuterungen zu den jeweiligen Antworten zu erfragen und festzuhalten. Der Einbürgerungsbewerber ist darauf hinzuweisen, dass unwahre Angaben als Täuschung der Einbürgerungsbehörde gewertet werden und – auch noch nach Jahren – zur Rücknahme der Einbürgerung führen können. Die Unterzeichnung der Bekenntnis- und Loyalitätserklärung nach Nr. 10.1.1.1 der vorläufigen Anwendungshinweise des BMI zum StAG bleibt unberührt; das Gleiche gilt für die Ergänzung zu Nrn. 8.1.2.5 und 9.1.2.1 der vorläufigen Anwendungshinweise.

1. Das Bekenntnis zur freiheitlichen demokratischen Grundordnung des Grundgesetzes für die Bundesrepublik Deutschland umfasst die Werteordnung des Grundgesetzes, die inhaltsgleich für alle Staaten der Europäischen Union gilt. Dazu gehören unter anderem
   - der Schutz der Menschenwürde
   - das Gewaltmonopol des Staates, das heißt, außer dem Staat darf in der Bundesrepublik Deutschland niemand Gewalt gegen einen anderen anwenden, es sei denn in Notwehr. Der Staat selbst darf Gewalt nur aufgrund einer gesetzlichen Ermächtigung anwenden
   - sowie die Gleichberechtigung von Mann und Frau.

   Entsprechen diese Grundsätze Ihren persönlichen Vorstellungen?

2. Was halten Sie von folgenden Aussagen?
   - „Demokratie ist die schlechteste Regierungsform, die wir haben, aber die beste, die es gibt."
   - „Die Menschheit hat noch nie eine so dunkle Phase wie unter der Demokratie erlebt. Damit der Mensch sich von der Demokratie befreien kann, muss er zuerst begreifen, dass die Demokratie den Menschen nichts Gutes geben kann ..."

3. In Filmen, Theaterstücken und Büchern werden manchmal die religiösen Gefühle von Menschen der unterschiedlichen Glaubensrichtungen verletzt. Welche Mittel darf der Einzelne Ihrer Meinung nach anwenden, um sich gegen solche Verletzungen seines Glaubens zu wehren, und welche nicht?

4. Wie stehen Sie zu Kritik an einer Religion? Halten Sie diese für zulässig? Setzen Sie sich damit auseinander?

5. In Deutschland können politische Parteien und Vereine wegen verfassungsfeindlicher Betätigung verboten werden. Würden Sie trotz eines solchen Verbots die Partei oder den Verein doch unterstützen? Unter welchen Umständen?

6. Wie stehen Sie zu der Aussage, dass die Frau ihrem Ehemann gehorchen soll und dass dieser sie schlagen darf, wenn sie ihm nicht gehorsam ist?

7. Halten Sie es für zulässig, dass ein Mann seine Frau oder seine Tochter zu Hause einschließt, um zu verhindern, dass sie ihm in der Öffentlichkeit „Schande macht“?

8. In Deutschland kann die Polizei bei gewalttätigen Auseinandersetzungen zwischen Eheleuten einschreiten und zur Abwehr von weiteren Gefahren den Täter für einige Tage aus der Wohnung verweisen? Was halten Sie davon?

9. Halten Sie es für einen Fortschritt, dass Männer und Frauen in Deutschland kraft Gesetzes gleichberechtigt sind? Was sollte der Staat Ihrer Meinung nach tun, wenn Männer dies nicht akzeptieren?

10. In Deutschland kann jeder bei entsprechender Ausbildung nahezu jeden Beruf ergreifen. Was halten Sie davon? Sind Sie der Meinung, dass bestimmte Berufe nur Männern oder nur Frauen vorbehalten sein sollten? Wenn ja, welche und warum?

11. Welche Berufe sollte Ihrer Meinung nach eine Frau auf keinen Fall ausüben? Hätten Sie bei bestimmten Berufen Schwierigkeiten, eine Frau als Autoritätsperson anzuerkennen?

12. In Deutschland kann jeder selbst entscheiden, ob er sich lieber von einem Arzt oder einer Ärztin behandeln lässt. In bestimmten Situationen besteht diese Wahlmöglichkeit jedoch nicht: Notfall, Schichtwechsel im Krankenhaus. Würden Sie sich in einem solchen Fall auch von einer Ärztin (männlicher Einbürgerungsbewerber) oder einem Arzt (Einbürgerungsbewerberin) untersuchen oder operieren lassen?

13. Man hört immer wieder, dass Eltern ihren volljährigen Töchtern verbieten, einen bestimmten Beruf zu ergreifen oder einen Mann ihrer Wahl zu heiraten. Wie stehen Sie persönlich zu diesem Verhalten? Was würden Sie tun, wenn Ihre Tochter einen Mann anderen Glaubens heiraten oder eine Ausbildung machen möchte, die Ihnen nicht gefällt?

14. Was halten Sie davon, dass Eltern ihre Kinder zwangsweise verheiraten? Glauben Sie, dass solche Ehen mit der Menschenwürde vereinbar sind?

15. In Deutschland gehört der Sport- und Schwimmunterricht zum normalen Schulunterricht. Würden Sie Ihre Tochter daran teilnehmen lassen? Wenn nein: Warum nicht?

16. Wie stehen Sie dazu, dass Schulkinder an Klassenausflügen und Schullandheimaufenthalten teilnehmen?

17. Ihre volljährige Tochter/Ihre Frau möchte sich gerne so kleiden wie andere deutsche Mädchen und Frauen auch. Würden Sie versuchen, dass zu verhindern? Wenn ja: Mit welchen Mitteln?

18. Bei *Einbürgerungsbewerberinnen:* Ihre Tochter möchte sich gerne so kleiden wie andere deutsche Mädchen und Frauen auch, aber Ihr Mann ist dagegen? Was tun Sie?

19. Ihre Tochter/Schwester kommt nach Hause und erzählt, sie sei sexuell belästigt worden. Was tun Sie als Vater/Mutter/Bruder/Schwester?

20. Ihr Sohn/Bruder kommt nach Hause und erzählt, er sei beleidigt worden. Was tun Sie als Vater/Mutter/Bruder/Schwester?

21. Erlaubt das Grundgesetz Ihrer Meinung nach, seine Religion zu wechseln, also seine bisherige Glaubensgemeinschaft zu verlassen und ohne Religion zu leben oder sich einer anderen Religion zuzuwenden? Was halten Sie davon, wenn man wegen eines solchen Religionswechsels bestraft würde (z. B. mit dem Verlust des Erbrechts)?

22. Sie erfahren, dass Leute aus Ihrer Nachbarschaft oder aus Ihrem Freundes- oder Bekanntenkreis einen terroristischer Anschlag begangen haben oder planen. Wie verhalten Sie sich? Was tun sie?

    (*Hinweis für die EBB:* Der Vorsitzende des Zentralrats der Muslime in Deutschland, Dr. Nadeem Elyas, hat im ZDF am 15. Juli 2005 – nach den Anschlägen in London – erklärt, die Zusammenarbeit mit den Sicherheitsbehörden sei für Muslime „ein islamisches Gebot und kein Verrat“!)

23. Sie haben von den Anschlägen am 11. September 2001 in New York und am 11. März 2004 in Madrid gehört. Waren die Täter in Ihren Augen Terroristen oder Freiheitskämpfer? Erläutern Sie Ihre Aussage.

24. In der Zeitung wird manchmal über Fälle berichtet, in denen Töchter oder Ehefrauen von männlichen Familienangehörigen wegen „unsittlichen Lebenswandels“ getötet wurden, um die Familienehre wieder herzustellen. Wie stehen Sie zu einer solchen Tat?

25. Was halten Sie davon, wenn ein Mann in Deutschland mit zwei Frauen gleichzeitig verheiratet ist?

26. Wie beurteilen Sie es, wenn ein verheirateter Mann aus Deutschland in seinen früheren Heimatstaat fährt und dort ein zweites Mal heiratet?

27. Manche Leute machen die Juden für alles Böse in der Welt verantwortlich und behaupten sogar, sie steckten hinter den Anschlägen vom 11. September 2001 in New York? Was halten Sie von solchen Behauptungen?

28. Ihre Tochter bewirbt sich um eine Stelle in Deutschland. Sie bekommt jedoch ein ablehnendes Schreiben. Später erfahren Sie, dass eine Schwarzafrikanerin aus Somalia die Stelle bekommen hat. Wie verhalten Sie sich?

29. Stellen Sie sich vor, Ihr volljähriger Sohn kommt zu Ihnen und erklärt, er sei homosexuell und möchte gerne mit einem anderen Mann zusammen leben. Wie reagieren Sie?

30. In Deutschland haben sich verschiedene Politiker öffentlich als homosexuell bekannt. Was halten Sie davon, dass in Deutschland Homosexuelle öffentliche Ämter bekleiden?

**Erklärung des Einbürgerungsbewerbers:**

Meine Antworten und Erläuterungen zu den gestellten Fragen sind korrekt wiedergegeben und entsprechen meiner tatsächlichen inneren Einstellung. Ich hatte keine Schwierigkeiten, die Fragen zu verstehen; soweit ich sie nicht gleich verstanden habe, wurden sie mir so erklärt, dass ich alles verstanden habe.

Ich wurde ausdrücklich darauf hingewiesen, dass unwahre Angaben als Täuschung der Einbürgerungsbehörde gewertet werden und – auch noch nach Jahren – zur Rücknahme der Einbürgerung führen können, selbst wenn ich dadurch staatenlos werden sollte.

Ort, Datum Unterschrift