20. Tätigkeitsbericht
des

Landesbeauftragten für Datenschutz

für die Jahre 2003 und 2004

dem Landtag und der Landesregierung
vorgelegt am 29.06.2005

(Landtagsdrucksache 13/460)

Der Landesbeauftragte
für Datenschutz Saarland
Roland Lorenz

Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Postfach 10 26 31, 66026 Saarbrücken
Tel.: 0681/94781-0, Fax: 0681/94781-29
E-Mail-Adresse: lfd-saar@t-online.de
Internet-Angebot unter www.lfd.saarland.de

Saarbrücken im Juni 2005

Geleitwort

Als seit Juni 2004 amtierender Landesbeauftragter für Datenschutz des Saarlandes obliegt es mir den 20. Tätigkeitsbericht meiner Dienststelle für die Jahre 2003 und 2004 vorzulegen.

Dies ist für mich eine faszinierende Aufgabe. Denn für einen langjährigen Steuerbeamten, also einen gelernten und langjährigen Datensammler ist diese Berichtslegung eine besondere Herausforderung, insbesondere an die eigene intellektuelle Redlichkeit.

Danken will ich an dieser Stelle dem Landtag des Saarlandes, seinem Präsidenten und seiner Verwaltung, die mich stets und jederzeit effektiv bei der Erfüllung meiner Aufgaben unterstützt haben. Dies hat bestimmend zum Erfolg meiner Arbeit beigetragen und war umso bedeutsamer, da im Jahre 2004 der Vorsitz der Konferenz der Beauftragten für Datenschutz des Bundes und der Länder vom Landesbeauftragten für Datenschutz des Saarlandes wahrgenommen wurde. Gerade durch die wohlwollende und bedingungslose Unterstützung des Landtages wurde der Konferenzvorsitz für meine Dienststelle und hiermit auch für das Saarland ein großer Erfolg.

Ebenfalls will ich hier meinem Vorgänger im Amte, dem nunmehrigen Direktor beim Landesrechnungshof des Saarlandes, Herrn Karl Albert, danken. Er hat in der überwiegenden Zeit des Berichtszeitraumes die Geschäfte des Landesbeauftragten für Datenschutz mit großem Engagement geführt und mir ein wohl geordnetes Haus überlassen.

Mein spezieller Dank gilt meinen Kolleginnen und Kollegen, die es mir durch ihren Einsatz, ihren Sachverstand und ihre Effizienz ermöglicht haben die Geschäfte des Landesbeauftragten erfolgreich zu übernehmen, den Vorsitz der Konferenz erfolgreich zu bewältigen und letztendlich diesen Bericht vorzulegen.

Zum Abschluss will ich dieses Geleitwort dazu nutzen, in vielleicht redundanter Weise ein in der datenschutzrechtlichen Diskussion immer wieder aufkommendes Tot-

schlagargument zu entkräften. Anlässlich der Verteidigung datenschutzrechtlicher Positionen wird als Gegenpunkt gewohnheitsmäßig gerne eingewandt, man habe ja nichts zu verbergen. Nun, das Selbstverständliche versteht sich von selbst, so sagt zwar der Volksmund. Wie er jedoch hinzufügt, es schadet nicht, wenn man das Selbstverständliche wiederholt. Daher die Feststellung:
Bei der datenschutzrechtlichen Diskussion und der Verteidigung datenschutzrechtlicher Grundsätze dreht es sich nicht darum, ob die Bürgerinnen und Bürger etwas zu verbergen haben. Es dreht sich allein und einfach darum, ob sie in verfassungsrechtlich zulässiger Weise Geheimnisse haben dürfen, egal vor wem, auch und insbesondere vor dem Staat.

Roland Lorenz
Landesbeauftragter für Datenschutz Saarland

Inhaltsverzeichnis

1 Vorbemerkung

Um Schwerpunkte bei der künftigen Arbeit festzulegen, um Akzente in der täglichen Arbeit einzubringen, ist es für mich als neuem Datenschutzbeauftragten unabdingbar notwendig gewesen, mir zunächst ein Bild über die Ist-Situation und darüber hinaus über die möglichen Perspektiven und daraus folgenden Handlungszwängen zu machen.

Nun, sowohl die saarländische Verfassung als auch das Grundgesetz verhelfen dem Datenschutz zu einem zweifelsohne nicht unbedeutsamen Gewicht. Diese Haltung schlägt sich auch bekanntlich im europäischen Recht und zwar in dem Entwurf eines Verfassungsvertrages und den einschlägigen europäischen Richtlinien nieder. Da wir uns als Bürgerinnen und Bürger und auch als politisch interessierte Menschen in den vergangenen und kommenden Wochen mit der europäischen Verfassung und ihrer Annahme beschäftigt haben und weiterhin beschäftigen werden, will ich unterstreichen, dass die europäische Grundrechtecharta mit ihrer Verankerung des Datenschutzes nunmehr Teil der EU-Verfassung geworden ist. Dies beweist, wie auch unter einer veränderten Großwetterlage die Implementierung des Datenschutzes im Interesse der Bürgerinnen und Bürger äußerste Bedeutung hat, behält und verwirklichbar bleibt.

Trotzdem kann nicht übersehen werden, dass das Grundrecht auf informationelle Selbstbestimmung, wie es vom Bundesverfassungsgericht in seinem Grundsatzurteil zur Volkszählung, sowie auch in einer Vielzahl weiterer Entscheidungen, ausgearbeitet wurde, offenkundig nicht länger Gegenstand eines einmütigen gesellschaftlichen und politischen Konsenses ist, wie er es bislang auf Grund unseres Verfassungs- und Gesellschaftsverständnisses sowie unseres Menschenbildes gewesen ist. Im Gegenteil, es kann hier nicht verdrängt werden, dass der Schutz des Rechts auf informationelle Selbstbestimmung breitflächig in Namen eines gleichwie verstandenen allumfassenden Sicherheitsbegriffs in Frage gestellt wird, ja offenkundig nach den Wünschen mancher gar diesem Sicherheitsbegriff ganz unterworfen werden soll.

Vor diesem Hintergrund werde ich ein besonderes Augenmerk auf den beabsichtigten beziehungsweise geforderten Ausbau staatlicher Informationsbefugnisse setzen. Denn nach den Anschlägen vom 11. September 2001 wurden und werden diese, wie auch die Erfolge bestimmter neuer Sicherheitstechniken, immer wieder zum Anlass genommen, eine Unzahl gesetzlicher Änderungen zu beschließen beziehungsweise zu fordern, mit denen jedenfalls die praktischen Möglichkeiten zur Überwachung der Bevölkerung ausgebaut und die Grundrechte, insbesondere das Grundrecht auf informationelle Selbstbestimmung tangiert werden könnten. Vor diesem Hintergrund werde ich wie in der Vergangenheit darauf achten, dass ein – jedenfalls scheinbar - monomanes Streben nach einer möglichst allumfassenden Sicherheit nicht die von Landesverfassung und Grundgesetz vorgegebenen Rechte überlagert. Ein demokratischer und freiheitlicher Rechtsstaat begegnet seinen Bürgerinnen und Bürgern nämlich mit dem grundsätzlichen Vertrauen, dass diese rechtstreu sind und sich auch entsprechend verhalten. Für staatliche Eingriffe bedarf es daher grundsätzlich zumindest eines Verdachts unrechtmäßiger Betätigung. Dieses Grundverständnis darf nicht umgekehrt werden. Ein auf kaltem Weg herbeigeführter Paradigmenwechsel ist nicht akzeptabel und müsste daher schon in den Ansätzen transparent gemacht und bekämpft werden.

Diese Sichtweise und das in der Vergangenheit gesetzte und für die Zukunft weiterhin zu setzende Schwergewicht sind, wie ich meine, eben ganz besonders im Lichte der beiden Entscheidungen des Bundesverfassungsgerichts zum sog. „Großen Lauschangriff“ vom 3. März 2004 unumgänglich. Diese Art die Entwicklung zu betrachten ist umso gebotener, als ja immer mehr menschliche Äußerungen und Tätigkeiten heute bereits in der virtuellen Welt der Netze stattfinden. Dort können Bürgerinnen und Bürger aufgrund der technischen Möglichkeiten jedoch potenziell einer qualitativ und quantitativ ganz anderen staatlichen Kontrolle ausgesetzt werden als in der realen Welt. Die stürmische Entwicklung der technologischen Rahmenbedingungen und Möglichkeiten hat für Datensammlung, Datenverarbeitung und Datenvernetzung Alternativen eröffnet, die bei Verabschiedung und Novellierung der einschlägigen Datenschutzgesetze nicht einmal im Ansatz vorstellbar waren. Ein Ende dieser Entwicklung ist nicht zu erwarten. Aus den bereits existierenden Dateien ließen sich ohne große Schwierigkeiten sowohl Anschauungen als auch Verhaltensweisen und Bestrebungen der Bürgerinnen und Bürger herauslesen. Auch erwecken die beste-

henden Dateien immer wieder neue Begehrlichkeiten. Die potenziell mögliche Verquickung von Dateien bzw. der Wunsch nach Aufhebung der bestehenden Zweckbindungen führen daher zu immer neuen Forderungen.

Den gläsernen Bürger gibt es nämlich potenziell schon, obwohl er sich breitflächig dessen nicht bewusst zu sein scheint, vielleicht weil es ihn auf Grund eintretender Gewöhnung möglicherweise immer weniger stört. Daher ist es für meine Dienststelle und mich mehr denn je von Bedeutung aufmerksam zu verfolgen, ob die Bewältigung der Herausforderungen unserer Zeit und der unserer Zeit nachgesagten Gefahren stets verfassungskonform und ohne Übermaß erfolgt.

Hierbei verkenne ich nicht, dass – wie von meinen Vorgängern erfolgreich praktiziert - durch angemessene und verfassungskonforme Abwägung der Ausgleich zwischen der wirksamen Erfüllung staatlicher Aufgaben und der Wahrung der individuellen Persönlichkeits- und Freiheitsrechte des Einzelnen, die sich eben auch im Grundrecht auf informationelle Selbstbestimmung konkretisieren, angestrebt, gefunden und umgesetzt werden muss. Da ich jedoch festgestellt habe, dass die Belange des Datenschutzes von den öffentlichen Stellen unseres Landes ernst genommen und praktiziert werden, blicke ich trotz alledem gerade diesbezüglich mit einer gewissen Gelassenheit in die Zukunft.

2 Technisch-organisatorischer Datenschutz

2.1 Hinweise des Ministeriums für Bildung, Kultur und Wissenschaft zu Rechtsfragen in Internet-Angeboten der Schulen mit Merkblatt des LfD „Schulen ans Netz mit Sicherheit“

Aus dem schulischen Bereich erreichen mich immer wieder Anfragen von Lehrern und Eltern zu Rechtsfragen bei der Darstellung der Schule in Internet-Homepages. Dabei musste ich auch feststellen, dass mein Merkblatt „Schulen ans Netz mit Sicherheit“ (siehe auch 19. TB, Ziffer 2.10) bei den zuständigen Lehrern oft unbekannt war und auch über die Fortbildungen des Landesinstituts für Pädagogik und Medien noch keine große Verteilung gefunden hatte.

Um diesbezüglich für eine bessere Verbreitung zu sorgen, wandte ich mich an das Ministerium für Bildung, Kultur und Wissenschaft, das den Gedanken gerne aufgriff, zumal gerade der Schulausschuss der Kultusministerkonferenz ein Muster „Rechtliche Hinweise zur Nutzung des Internet an Schulen“ erarbeitet hatte, in dem datenschutzrechtliche Fragen vergleichsweise knapp behandelt wurden. In Abstimmung mit dem Ministerium wurden diese Hinweise auf die Belange des Saarlandes zugeschnitten und mein Merkblatt integriert. Der gesamte Text wurde im Gemeinsamen Ministerialblatt des Saarlandes veröffentlich und erreichte so alle Schulen (GMBl 2003 S. 293, S. 518).

In einem zweiten Schritt wurde in Abstimmung mit dem Ministerium und dem Hochwaldgymnasium Wadern eine Muster-Internet-Ordnung erarbeitet, die den Schulen zur Anpassung zur Verfügung gestellt wurde. Die Hinweise und die Muster-Ordnung wurden vom Ministerium auch auf dem Bildungsserver für den allgemeinen Abruf bereitgestellt.

2.2 Schul-Homepages und Impressum mit Internet-Rechtsgenerator, Wettbewerb „Computer-Lotsen“

Im Rahmen der datenschutzrechtlichen Prüfung von Schul-Homepages wurde immer wieder deutlich, dass zur Anbieterkennzeichnung (Impressum) nach Teledienstgesetz und Mediendienste-Staatsvertrag Unsicherheiten bezüglich der korrekten Form bestanden. Dazu hatte das Projekt „Remus“ des Lehrstuhls für Rechtsinformatik der Universität Saarbrücken die Rechtsauffassung vertreten, die auch in der Handreichung „Die Schulhomepage“ von „Schulen ans Netz“/„Lehrer-Online“ umgesetzt worden war, dass als Anbieter von Schul-Homepages der jeweilige Schulträger verantwortlich zeichnen müsse. Dies hätte zur Folge gehabt, dass die Schul-Homepages und ihre Inhalte von der jeweiligen Gemeindeverwaltung hätten geprüft und vom Bürgermeister freigegeben werden müssen und insofern der Infrastruktur wie Möbel oder Räume gleichgestellt wären. In Abstimmung mit dem Ministerium und dem Lehrstuhl für Rechtsinformatik konnte schließlich geklärt werden, dass das Impressum eher dem pädagogischen Verantwortungsbereich zuzuordnen ist und insofern das Ministerium für Bildung, Kultur und Wissenschaft letztendlich verantwortlich ist.

Nach Klärung dieser Rechtsfrage erarbeitete die Gesamtschule Sulzbachtal in Dudweiler in einem Schülerprojekt einen „Internet-Rechtsgenerator“, ein Programm, das mit Hilfe von im Dialog abgefragten Daten der Schule ein solches Muster-Impressum automatisch erstellt, wobei auch die Besonderheiten von Privatschulen berücksichtigt wurden. Dankenswerterweise wurde die Projektarbeit noch dahingehend erweitert, dass der Rechtsgenerator auch eine mit mir abgestimmte Datenschutz-Info (Online-Privacy-Policy) erzeugt, die von den Schulen ergänzend integriert werden kann. Der Rechtsgenerator und das Muster-Impressum wurden vom Ministerium im Bildungsserver veröffentlicht.

Mehrere saarländische Schulen hatten sich an einem bundesweiten Wettbewerb „Schüler als Computer-Lotsen 2002/2003“ beteiligt und entsprechende Internet-Angebote erstellt. Ziel dieses Wettbewerbs war, Schüler als Computer-Lotsen zu gewinnen, die dann andere Mitschüler-/innen dabei unterstützen sollten, fachgerecht mit dem PC umzugehen. Dabei sollten sie ein konkretes Multimedia-Projekt (in der

Regel ein Internet-Angebot) durchführen und ihr Wissen weiter geben. Bei der datenschutzrechtlichen Prüfung dieser Angebote musste ich feststellen, dass dabei Arbeiten ausgezeichnet worden waren, bei denen die Jury offensichtlich rechtliche (z. B. ein korrektes Impressum) und datenschutzrechtliche Aspekte (Umfang personenbezogener Daten) nicht berücksichtigt hatte; es stand wohl vor allem das Layout als Bewertungskriterium im Vordergrund. Sogar die Homepage des Projektbüros hatte kein korrektes Impressum. Damit auch die rechtlichen und vor allem datenschutzrechtlichen Aspekte in diese Vermittlungsarbeit einfließen konnten und dann auch bei der Weitergabe nichts Falsches vermittelt wurde, habe ich alle beteiligten Schulen und auch das Wettbewerbsbüro kontaktiert und auf die Hinweise des Ministeriums zu Rechtsfragen im Internet und unser Merkblatt „Schulen ans Netz mit Sicherheit“ hingewiesen. Erstaunt musste ich feststellen, dass einige verantwortliche Lehrer die Hilfen und Hinweise nicht gerne aufgreifen wollten und sie sogar als Einmischung in ihre pädagogische Verantwortung ansahen.

2.3 MBKW: Handreichung Projekt EMSIS „E-Mail für die Schulverwaltung“

Im Zuge der Qualifizierung von Lehrern für den Einsatz neuer Medien im Unterricht hatte das Landesinstitut für Pädagogik und Medien eine Handreichung zur E-Mail-Nutzung in der Schulverwaltung im Saarland erarbeitet und an alle Schulen verteilt. Bei der Prüfung dieser Unterlage fiel mir auf, dass das Papier vorrangig Kenntnisse und Fertigkeiten zur Nutzung der E-Mail-Funktionalität vermittelte, aber Risiken der Nutzung und datenschutzrechtliche Fragen nicht betrachtete. In Abstimmung mit dem verantwortlichen Autor habe ich dann einen zweiten Teil dieser Handreichung entworfen, mit dem die fehlenden Aspekte ergänzt wurden. Auch dieser zweite Teil wurde an die Schulen versandt und wird im Rahmen der Lehrerfortbildung genutzt. Außerdem hat ihn das Ministerium für Bildung, Kultur und Wissenschaft im Bildungsserver für den allgemeinen Zugriff zur Verfügung gestellt.

2.4 Datenschutzrechtliche Prüfung des Landessportverbandes (LSVS)

Im Zuge der datenschutzrechtlichen Behandlung einer Auskunft zu den Fortbildungsmaßnahmen des Landessportverbandes wurde deutlich, dass bei dessen Mitarbeitern Unsicherheiten bezüglich der geltenden datenschutzrechtlichen Bestimmungen vorhanden waren. Durch eine Querschnittsprüfung sollten eventuelle Probleme erkannt und eine entsprechende Fortbildung der Mitarbeiter auf den Weg gebracht werden.

Dank der Unterstützung durch den Präsidenten und die Geschäftsführung war die Prüfarbeit weitgehend problemlos und wurde von den Mitarbeitern unterstützt; allerdings musste an einigen Stellen doch noch Überzeugungsarbeit geleistet werden.

Geprüft wurden ausgewählte Schwerpunkte im Bereich der technischen und organisatorischen Maßnahmen für Datenschutz und Datensicherheit, wobei auch Kontakt mit dem Personalrat gesucht wurde. Ein wichtiger Aspekt dabei war das Internet-Angebot des LSVS, das schon während der Prüfung aus datenschutzrechtlicher Sicht angepasst wurde sowie der Einsatz der Informationstechnik. Weitere Aspekte der Prüfung waren:

- Sichere Aufbewahrung von Personalakten und Gleitzeitdaten
- Vernichtung von nicht mehr benötigten Akten
- Risikoanalyse und IT-Sicherheitskonzept mit Notfallvorsorge
- IT-Dienstanweisung
- Beteiligung des LfD vor der Freigabe neuer Verfahren
- Schulung der Mitarbeiter zum Datenschutz
- Datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung und Beteiligung des LfD.

Der LSVS hat sich bereit erklärt, die im Prüfbericht genannten Forderungen so weit wie möglich zu erfüllen und die Ergebnisse der datenschutzrechtlichen Prüfung in ihren Grundzügen auch den angegliederten Fachverbänden zur Verfügung zu stellen, da diese als eingetragene Vereine wie auch die zu den jeweiligen Verbänden gehörenden Vereine nicht meiner Kontrolle unterliegen. Dies wurde auch von der

dafür zuständigen Datenschutzaufsicht beim Ministerium für Inneres und Sport begrüßt.

2.5 eGovernment-Plattform der Landesverwaltung

Die Landesverwaltung unternimmt große Anstrengungen den saarländischen Bürgerinnen und Bürgern und der Wirtschaft, aber auch den Verwaltungen untereinander die Abwicklung formulargebundener Verwaltungsvorgänge zu erleichtern und eine elektronische Kommunikation zu ermöglichen. Nach einem Start des eGovernment-Projekts „Behördendienste Saar“ für vernetzte Dienstleistungen mit Schwerpunkt „Formularserver“ und unter Beteiligung von Pilotgemeinden ist das Konzept inzwischen auf ein „elektronisches Bürgerportal“ mit einem Behördenführer und Lebenslagenmodell ausgeweitet worden. Der Saarländische Städte- und Gemeindetag sowie der Landkreistag haben einen Zweckverband „Elektronische Verwaltung für saarländische Kommunen - eGo-Saar“ gebildet und sich mit dem Land zu einer Initiative „e-Government-Portal“ zusammengeschlossen. Meine datenschutzrechtlichen Vorschläge zum eGo-Saar-Kooperationsvertrag wurden dankenswerterweise vollständig übernommen. Meine Vorschläge für eine IT-Dienstanweisung zur E-Mail- und Internet-Nutzung sollen entsprechend berücksichtigt werden.

Das saarländische Verwaltungsverfahrensgesetz wurde um die Möglichkeit der elektronischen Kommunikation mit Absicherung durch eine qualifizierte elektronische Unterschrift ergänzt. In Konsequenz daraus muss die öffentliche Verwaltung in der Lage sein, von den Bürgern signierte Dokumente auch angemessen entgegennehmen und die notwendigen Schritte sicher abwickeln zu können. Wegen des hohen Kostenumfangs, der für jede Dienststelle anfallen würde, soll als Übergangslösung der Empfang digital signierter Post und die entsprechende Bearbeitung und Weiterleitung durch Einrichtung einer zentralen virtuellen Poststelle im Saarland realisiert werden.

Aus Sicht des Datenschutzes liegen meine Schwerpunkte in einer sicheren, datenschutzgerechten IT-Infrastruktur und Internet-Nutzung. Bei der Verwendung personenbezogener Daten in Formularen und Datenbanken sind die Aspekte Rechtmäßigkeit und als deren Inhalt insbesondere die Erforderlichkeit sowie die Absicherung des

Datentransfers über das Internet angemessen umzusetzen. Bürger und Verwaltung erwarten, dass mit der Nutzung von eGovernment-Dienstleistungen keine Einschränkungen der Vertraulichkeit und Integrität ihrer Daten verbunden sind und die Verbindlichkeit des Verwaltungshandels gesichert bleibt. Neben den üblichen Standard-Maßnahmen zur IT-Sicherheit kommen dazu nun verstärkt Technologien zur Verschlüsselung und elektronischen Unterschrift zur Anwendung, wobei viele Bürgerinnen und Bürger sowie auch Bedienstete mit dem Einsatz dieser Technologien Schwierigkeiten haben dürften. Auch hier kann die virtuelle Poststelle die sichere elektronische Kommunikation erleichtern. Die Datenschutzbeauftragten des Bundes und der Länder haben dazu eine Handreichung „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ herausgegeben und im Rahmen der im Oktober 2003 in Saarbrücken stattgefundenen Datenschutzkonferenz zur Anwendung empfohlen. Ich werde die Umsetzung dieser Empfehlungen entsprechend begleiten.

2.6 Überarbeitung der IT-Dienstanweisungen der Ressorts nach SDSG-Novellierung

In der Vergangenheit hatten die Obersten Landesbehörden und ihre nachgeordneten Dienststellen den Einsatz der Informationstechnik mit einer IT-Dienstanweisung geregelt, die auf mit mir abgestimmten Mustern beruhte.

Nach der Änderung des Saarländischen Datenschutzgesetzes im Jahre 2002 bestand nun ein Überarbeitungsbedarf, vor allem hinsichtlich der neu eingeführten Vorabkontrolle und der Bestellung und Aufgabenzuordnung von behördlichen Datenschutzbeauftragten. Mit einem Schreiben forderte ich Ende 2002 die Obersten Landesbehörden auf, ihre Dienstanweisung entsprechend anzupassen und die ernannten Datenschutzbeauftragten zu melden. Bei der Überarbeitung der Dienstanweisungen habe ich meine Unterstützung angeboten, um auch dieses Mal ein Muster empfehlen zu können. Inzwischen haben lediglich das Ministerium der Finanzen und das Ministerium für Umwelt eine mit mir abgestimmte Fassung in Kraft gesetzt. Die Überarbeitungsbemühungen der anderen Ressorts sind jetzt durch die Ressort-Neubildung ins Stocken geraten. Ich gehe aber davon aus, dass sie noch im laufen-

den Jahr 2005 zu Ende gebracht und dann auch die nachgeordneten Dienststellen entsprechend unterstützt werden.

2.7 Datenschutzaspekte im Bereich der Universität des Saarlandes

2.7.1 Internet-Angebot und Projekt „Virtuelle Saar-Universität (VISU)“

Ende des Jahres 2003 wurde ich zufällig auf ein bevorstehendes „Relaunch“ der Internet-Seiten des Projekts „Virtuelle Saar-Universität“ aufmerksam. Bei der Überprüfung der Seiten fand ich, wie erwartet, eine Präsentation von personenbezogenen Daten wie z. B. Referenten, Preisträger, Beiratsmitglieder und Experten vor und erhielt auf meine Anfrage hin den Bescheid, es handele sich dabei gar nicht um personenbezogene Daten. Nach Hinzuziehung des kommissarischen Datenschutzbeauftragten der Universität gelang es dann, die Verantwortlichen von der Existenz solcher Daten und der Relevanz der entsprechenden Bestimmungen des Saarländischen Datenschutzgesetzes zu überzeugen. Das Internet-Angebot wurde danach datenschutzgerecht umgestaltet und entsprechende Einwilligungserklärungen zur Veröffentlichung personenbezogener Daten eingeholt. Auch dieses Projekt macht, wie schon andere zuvor, deutlich, dass bei den Studierenden und Bediensteten der Universität Nachhol- bzw. Schulungsbedarf bezüglich der geltenden Bestimmungen des Saarländischen Datenschutzgesetzes besteht.

2.7.2 Dienstvereinbarung/Dienstanweisung zur Internet- und eMail-Nutzung

Schon im Jahre 1998 wurde ich mit dem Problem der erlaubten bzw. zumindest geduldeten privaten Internet- und E-Mail-Nutzung von Mitgliedern der Universität befasst. Mein Vorschlag, mit Hilfe einer entsprechenden Dienstanweisung oder durch Ergänzung der Benutzerordnung für das Rechenzentrum der Universität die rechtlichen und technisch-organisatorischen Fragen zu regeln, wurde aufgegriffen und eine Projektgruppe gebildet. Trotz mehrerer Besprechungen gelang es auch im Jahre

1999 und im Folgejahr nicht, die Problematik einer angemessenen Regelung zuzuführen. Eine gewisse Verzögerung entstand dann dadurch, dass die saarländische Landesverwaltung im Jahre 2000 in einer Arbeitsgruppe zur Erarbeitung einer gemeinsamen Geschäftsordnung für oberste Landesbehörden (GGO) die Aspekte einer privaten E-Mail- und Internet-Nutzung beleuchten und entsprechende Regelungen vorlegen wollte. Bis zu dieser Vorlage wollten die Uni-Gremien keine weiteren Schritte mehr für einen eigenen Entwurf unternehmen. In diesem Zusammenhang habe ich eine (datenschutz-)rechtliche Bewertung der privaten E-Mail- und Internet-Nutzung erarbeitet und den zuständigen Gremien zugeleitet. Die GGO der Landesverwaltung wurde schließlich verabschiedet und im Gemeinsamen Ministerialblatt des Saarlandes am 16.10.01 veröffentlicht. Wegen der damit verbundenen Rechtsfolgen enthält sie ein Verbot der privaten Nutzung. Nachdem auch im Jahre 2002 keine weiteren Aktivitäten seitens der Uni erkennbar waren, versuchte ich Anfang 2003 das Problem einer erneuten Lösung zuzuführen. Die Uni-Verwaltung legte dann den Entwurf einer IT-Nutzungsordnung für die Universität und einer IT-Dienstvereinbarung für die private Internet-Nutzung vor, in der die private Nutzung mit Blick auf einen entsprechenden Entwurf des Bundesbeauftragten für den Datenschutz unter bestimmten Bedingungen zugelassen werden sollte. Auf meine Stellungnahme vom 30.09.2003 steht noch jede weitere Reaktion aus.

2.7.3 Der behördliche Datenschutzbeauftragte der Universität

Bei den genannten und weiteren kleineren Projekten wurde immer wieder deutlich, dass die vielen Projekte der Universität nicht mit den beschränkten Kapazitäten meiner Dienststelle betreut werden können. Auch ist ein lokal verfügbarer Ansprechpartner schneller und einfacher zu erreichen. Auf meinen Hinweis hin hat die Universitätsleitung inzwischen einen eigenen behördlichen Datenschutzbeauftragten bestellt, der auch als mein Ansprechpartner und Moderator bei datenschutzrechtlichen Fragen fungiert.

2.8 Checkliste Vorabkontrolle

In § 11 Abs. 1 SDSG ist geregelt, dass im Rahmen einer Vorabkontrolle vor dem erstmaligen Einsatz automatisierter Verfahren zur Verarbeitung von personenbezogenen Daten zu prüfen ist, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können.

Auf Anfrage des Ministerium für Umwelt hin, das die Vorgehensweise einer solchen Vorabkontrolle in seine IT-Dienstanweisung aufnehmen wollte, habe ich dann eine Checkliste zur Vorabkontrolle entwickelt, mit deren Hilfe der für diese Arbeiten zuständige behördliche Datenschutzbeauftragte in die Lage versetzt wird, die gesetzlichen Anforderungen zu erfüllen. Zusätzlich ist die Checkliste so ausgelegt, dass mit ihr alle Daten und Angaben erarbeitet werden, die später in der nach § 9 SDSG erforderlichen Verfahrensbeschreibung enthalten sein müssen. Die Checkliste zur Vorabkontrolle wurde auch in meinem Internet-Angebot für den allgemeinen Abruf bereitgestellt.

2.9 Risiken aus USB-Schnittstellen und PDA

Heutige Computer sind mit sogenannten USB-Schnittstellen (Universal Serial Bus) ausgestattet. Zu Anfang wurden diese Anschlüsse genutzt, um Drucker, Tastaturen und Mäuse zu betreiben. Hilfreich an diesen Schnittstellen war auch, dass sie die angeschlossenen Geräte mit Strom versorgen und diese im laufenden Betrieb angeschlossen und abgehängt werden können.

Inzwischen wird die Schnittstelle auch für den Anschluss von Peripheriegeräten wie Disketten-, CD-ROM-, DVD-, Festplattenlaufwerken, Modems, Netzwerk- und Videoadaptern und vor allem von Speichergeräten wie z. B. USB-Sticks, Digital-Kameras und auch für den Anschluss von Computern wie z. B. PDA´s (Personal Digital Assistent) genutzt. War bei Systemen mit älteren Betriebssystemen noch die Installation geeigneter Treiber erforderlich, erkennen neuere Betriebssysteme wie Windows-XP solche Geräte automatisch und aktivieren die notwendigen Treiber beim Einstecken.

Mit solchen USB-Sticks, die zum Teil nicht größer als ein 2-Euro-Stück und sogar in Uhren, Taschenmessern oder Kugelschreibern eingebaut sind und Personal Digital Assistants (PDA´s), deren Speicherkapazität inzwischen im Gigabyte-Bereich angekommen sind, sowie mit externen Festplatten, deren Kapazitäten bis zum Terabyte-Bereich reichen, sind hohe Risiken für Datenbestände und Programme und sogar Betriebssysteme hinzugekommen. Es ist nicht nur möglich, Datenbestände und Programme unerkannt zu kopieren, sondern auch separate Betriebssysteme und Programme auf diesen Speichern zu starten und damit die laufenden Systeme zu überlisten bzw. zu korrumpieren. Gerade bei PDA´s wird oft eine Anschlussmöglichkeit gewünscht, da diese zur Synchronisierung von Terminen, Mails und Dokumenten mit anderen Systemen gekoppelt werden.

Um diesen Risiken begegnen zu können, sollten USB-Schnittstellen entweder ganz deaktiviert, oder mit geeigneter Software bzw. Konfiguration des Betriebssystems auf zulässige Funktionalitäten hin überwacht werden. Auch das Booten von der USB-Schnittstelle sollte standardmäßig deaktiviert werden. Wird der Anschluss von PDA´s zur Synchronisation gestattet, sollten die betroffenen Mitarbeiter intensiv auf das damit verbundene Risiko hingewiesen und durch geeignete Kontrollen mögliche missbräuchliche Nutzungen erkannt werden. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder hat in der Orientierungshilfe „Datensicherheit bei USB-Geräten“ die Problematik näher dargestellt und konkrete technische Maßnahmen beschrieben, um einen Missbrauch von USB-Geräten weitgehend ausschließen zu können. Diese Orientierungshilfe ist in meinem Internet-Angebot abrufbar.

2.10 Risiken aus RFID

Große Warenhauskonzerne haben damit begonnen, ihre Produkte mit sogenannten RFID-Tags (Radio Frequency Identification) auszustatten, die die bisherigen Barcode-Etiketten ablösen sollen. Mit Hilfe dieser Tags sollen die Warenströme besser gesteuert, die Inventur erleichtert und das Diebstahlrisiko minimiert werden.

RFID-Tags sind Mikroprozessoren mit Speicher und einer Antenne, die in der Regel nicht nur zum Datenaustausch, sondern auch zur Stromversorgung des integrierten Chips dient und mit Hilfe geeigneter Lesegeräte kontakt- und berührungslos aktiviert werden können. Eine manuelle Handhabung der Waren ist dann nicht mehr erforderlich und es können ganze Paletten oder Einkaufskörbe mit ihren einzelnen Artikeln im Vorbeifahren registriert werden. Auch Fahrscheine und Eintrittskarten (wie z. B. zur Fußballweltmeisterschaft) sollen mit solchen Tags gesichert und leichter handhabbar werden. Es wird sogar erwogen, Ausweise und Geldscheine damit auszustatten, so dass die Echtheit der Dokumente und Geldscheine erkannt und die darin enthaltenen Daten automatisch überprüft werden können. Solche Tags können auch, unter die Haut gepflanzt, die bei der Tierzucht üblichen Ohrmarken ersetzen und es hat offensichtlich auch schon Menschen gegeben, die sich die Chips unter die Haut haben legen lassen, damit ihre Daten wie z. B. Name, Adresse und die Blutgruppe auch dann abrufbar und sicher identifizierbar sind, wenn sie entführt wurden oder ohnmächtig geworden sind. Wichtige Dokumente und Gegenstände wie sie in Archiven, Museen, Bibliotheken oder Bildergalerien aufbewahrt werden, könnten so identifizierbar gemacht und ein Verlegen oder ein Diebstahl leicht erkannt werden. Höherwertige Tags können sogar einen zusätzlichen Kryptoprozessor für komplexe Verschlüsselungsverfahren und beschreibbare EEPROM-Speicher enthalten, auf denen beliebige Nutzer-Daten, auch personenbezogene, gespeichert werden können. Nachträglich könnte sogar ein neues Betriebssystem mit für den Nutzer unbekannten Funktionen aufgespielt werden.

Derzeit besteht das technische Problem der RFID-Tags noch in den relativ hohen Kosten der Chip-Herstellung in Ätz-Technik, so dass die Ausstattung kleinerer Objekte wie z. B. Rasierklingenpackungen damit noch zu teuer ist. Neuere Entwicklungen zeigen jedoch Möglichkeiten auf, die Tags per Druck und damit sehr kostengünstig zu erzeugen.

Es liegt auf der Hand, dass solche technischen Möglichkeiten auch missbraucht werden können. So kann das Warenhaus die Daten des für Rabattzwecke ausgestellten Kundenausweises und die gekauften Waren zur Bildung von Kundenprofilen nutzen. Beim Betreten des Kaufhauses kann der Kunde erkannt, mit Namen begrüßt und auf das auf seine Kaufinteressen passende Sonderangebot im dritten Laufgang hinge-

wiesen werden. Beim Passieren der Kasse können die Systeme automatisiert alle Waren im Einkaufswagen registrieren und den Kassenbon auswerfen. Im Reklamationsfalle könnte die gekaufte Ware Zeitpunkt, Preis und Verkäufer sowie die ursprünglichen Daten der Produktion mitteilen. Diebe könnten die Geldbörse eines Passanten zuvor scannen, um zu erfahren, ob sich ein Diebstahl oder Überfall überhaupt lohnt. Vom Kunden getragene Kleidung und in der Tasche befindliche Gegenstände könnten auf das finanzielle Potential des Kunden, sein Spektrum an Einkaufsmöglichkeiten und die Nutzungsfrequenz von Konkurrenten hin ausgewertet werden. Durch die Auswertung vieler Scanner-Daten könnte ein Bewegungsprofil erstellt werden. Neben dem Verlust weitgehender Anonymität kommt auch das Risiko hinzu, dass der Bürger die Nutzung dieser Technik nicht bemerkt und damit nicht mehr weiß, wer welche Daten zu welchem Zweck verarbeitet. Sind derzeit noch Funkreichweiten von wenigen Zentimetern als eine gewisse Absicherung anzusehen, hängt es von den genutzten Frequenzen, der Empfindlichkeit des Empfängers und des Transponders ab, ob RFID-Tags nicht auch über mehrere Meter hinweg aktiv sein und zumindest die Daten gelesen werden können. Die Kommunikation kann unbefugt mitgelesen, die Daten auf den Chips manipuliert oder gar gelöscht oder der Datentransfer blockiert werden.

Neben der Verschlüsselung der Daten, Authentifizierung der zulässigen Lesegeräte und Löschung der Daten bzw. Deaktivierung der Funktionalität kommen als Sicherungsmaßnahmen strafbewehrte Nutzungsverbote und beschränkte Nutzungsmöglichkeiten in Betracht, bei denen der Kunde bewusst aktiv werden muss, bevor die Kommunikation überhaupt frei gegeben wird. Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung (Anlage 15.18) einen transparenten Umgang mit dieser Technologie gefordert, bei dem auch künftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit bei personenbezogenen Daten sichergestellt werden kann. Auch beim Einsatz von miniaturisierten und in Produkte eingebetteten IT-Systemen muss das Recht auf informationelle Selbstbestimmung gewährleistet bleiben.

2.11 Risiken der Knoppix-CD

Seit einigen Monaten liegen den Computerzeitschriften sogenannte Knoppix-CD´s bei, die ein lauffähiges Linux-Betriebssystem enthalten. Ein entscheidender Vorteil dieser Lösung besteht darin, dass das Linux-System, ein zum Booten zugelassenes CD-/DVD-Laufwerk vorausgesetzt, sich komplett in den Hauptspeicher lädt und keine Installation auf dem vorhandenen PC-System erforderlich ist. Innerhalb dieses Linux-Betriebssystems kann auf der CD vorhandene Software genutzt und z. B. mit Open-Office Dateien bearbeitet und auch Peripheriegeräte wie Drucker angesprochen werden. Auch sind ein Mail-Abruf und ein Internet-Surfen möglich. Geworben wird für diese Lösung auch mit der Möglichkeit, von einem per se sauberen System ein Virenscannen auf dem möglicherweise infizierten Windows-System zu starten oder sogar Fehler und Probleme im Windows-System von außen zu reparieren. Nach Beendigung des Linux-Systems ist dessen Nutzung auf dem vorhandenen PC-System nicht feststellbar. Die CD wird für alle empfohlen, die einmal Erfahrungen mit Linux machen wollen, ohne deswegen eine Parallel- oder gar Ersatzinstallation vornehmen zu müssen.
Riskant an dieser so attraktiven Lösung sind jedoch neben den oben genannten Virenscan- und Reparaturmöglichkeiten auch die auf der CD vorhandenen weiteren Funktionalitäten. So ist es unter Anderem möglich, auf einem vorhandenen Windows-System Programme und sogar Word-Dateien zu lesen, zu modifizieren oder per Internet zu versenden. Das gilt auch für Windows-XP-Systeme, die ihren Start mit Benutzerkennung und Passwort schützen, gegenüber dem Knoppix-Linux aber völlig offen sind. Mit Hilfe von Netzwerktools ist es möglich, den Netzwerk-Traffic lokaler Netze und von Funknetzen mitzulesen und zu manipulieren. Diese Lösungen, propagiert für Netzwerkadministratoren, die damit Lücken ihrer Installation finden und beheben können sollen, sind aber auch nutzbar für jeden neugierigen oder sogar böswilligen Laien oder Hacker.

Zwar wird bezüglich dieses Risikos darauf hingewiesen, dass solche Software im Internet jederzeit beschaffbar ist und insofern ein schlauer Schüler oder Mitarbeiter sich ohne Probleme eine solche CD selbst zusammenstellen könnte. Doch war es noch nie so leicht wie mit dieser Knoppix-CD, die zumindest im Schülerkreise gerne

kopiert werden dürfte, ein lauffähiges System unerkannt zu starten und Daten der Mitschüler oder sogar einer arglosen Schulverwaltung zu lesen oder zu manipulieren, genauso wie dies ein neugieriger oder frustrierter Mitarbeiter machen kann. Das Einbruchswerkzeug wird sozusagen frei Haus geliefert.

In diesem Zusammenhang sei angemerkt, dass in Computer-Zeitschriften auch Anleitungen zu finden sind, wie solche bootbaren Linux-Varianten mit der genannten Anwendungssoftware auf USB-Speichern abzulegen sind, um die genannte Funktionalität auch mit USB-Speichern nutzen zu können.

Um solchen Risiken zu begegnen, sollten die Administratoren durch geeignete Konfiguration des BIOS oder des Betriebssystems bzw. durch Einsatz einer entsprechenden Überwachungssoftware ein Booten von Betriebssystemen von CD oder USB-Schnittstelle verhindern. Sehr hilfreich dabei ist auch eine Basis-Verschlüsselung des Betriebssystems, die z. B. bei der Installation von Windows-XP gewählt werden kann, womit auch der Gefahr eines Datenmissbrauchs bei Diebstahl oder Verlust von Laptops begegnet werden kann. Auf die Risiko-Beschreibung und geeignete Lösungen habe ich schon unter TZ 2.9 hingewiesen.

3 Übergreifende Themen

3.1 Anfragen privater Firmen zum Datenschutz

Meine Dienststelle erreichen häufig Anfragen privater Firmen, die ihre Produkte datenschutzgerecht gestalten möchten.

Ich weise regelmäßig darauf hin, dass mir eine Befassung mit den datenschutzrechtlichen Problemen Privater nicht gestattet ist, da ich ausschließlich für öffentliche Stellen zuständig bin. Erst wenn eine öffentliche Stelle definitiv beabsichtigt, das Produkt einer Firma auf vertraglicher Basis einzusetzen, kann ich mit rechtlicher oder technischer Beratung zur Verfügung stehen.

Die öffentlichen Stellen möchte ich daher darum bitten, Firmen grundsätzlich nicht den Rat zu geben, sich mit ihren Problemen vor diesem Zeitpunkt an mich zu wenden. Auch aus wettbewerbsrechtlichen Gründen verbietet es sich, Firmen durch die datenschutzrechtliche Beratung einen Vorteil gegenüber Mitkonkurrenten zu verschaffen, solange das Konkurrenzverhältnis noch besteht.

3.2 Gesetzgebungsvorhaben des Bundes

Zu Beginn der jetzigen Legislaturperiode des Bundestages haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 15.1) Bilanz gezogen, um immer noch ausstehende Gesetzgebungsvorhaben des Bundes erneut in Erinnerung zu rufen.

An allererster Stelle sei hier die Modernisierung des Bundesdatenschutzgesetzes zu erwähnen, dessen zweite Novellierungsstufe noch nicht in Angriff genommen wurde. Herausgreifen möchte ich dazu die von Anfang an umstrittene Bestimmung zur Videoüberwachung (§ 6 b), die neben den privaten Stellen und Bundesbehörden auch auf öffentlich-rechtliche Unternehmen des Landes, die am Wettbewerb teilnehmen,

Anwendung findet (§ 2 Abs. 2 SDSG). Statt – wie vom Gesetzgeber beabsichtigt – einer tatsächlichen Begrenzung der Videoüberwachungen zu dienen, hat die Normierung in der Realität zu einem ausufernden Wildwuchs dieser Technik geführt (vgl. TZ 14.9). Das gesetzgeberische Ziel kann damit nicht als erreicht gelten.
An zweiter Stelle möchte ich die Stärkung einer unabhängigen, effizienten Datenschutzkontrolle hervorheben, die im privaten Bereich durch die Fachaufsicht – auch wenn sie tatsächlich nicht ausgeübt wird – nicht den Vorgaben nach Art. 28 der EG-Datenschutzrichtlinie entspricht. Im Rahmen der zweiten Stufe der Novellierung des BDSG sollte auch diese Schieflage zurechtgerückt werden.

Wenn auch das eine oder andere Thema in der laufenden Legislaturperiode aufgegriffen wurde (z.B. Diskussionsentwurf eines Gendiagnostikgesetzes), so sind dennoch zahlreiche andere (z.B. Arbeitnehmerdatenschutz, Datenschutz im Steuerrecht, Datenschutz bei der Terrorismusbekämpfung) entweder gänzlich ungeregelt geblieben oder nicht zufrieden stellend normiert.

Durch die Modernisierung des Bundesdatenschutzgesetzes und durch den Konsens auf die dann weitgehende Anwendbarkeit fortschrittlicher Regelungen des BDSG auch im bereichsspezifischen Datenschutzrecht könnte ein großer Fortschritt in der Verständlichkeit und Vereinfachung des Datenschutzes erzielt werden.

3.3 Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Nach der Entscheidung des Bundesverfassungsgerichts in seinem Urteil zur strategischen Fernmeldeüberwachung haben die Datenschutzbeauftragten des Bundes und der Länder die zuständigen Stellen aufgefordert, die für alle besonders eingriffsintensiven Erhebungen geltende Kennzeichnung der Daten zur Wahrung gesetzlicher Zweckbindungen zu vollziehen (Anlage 15.4).

Nicht nur bei Eingriffen in das Fernmeldegeheimnis ist den daraus gewonnenen Daten im Laufe der Datenverarbeitung, insbesondere nach der Datenübermittlung, nicht mehr anzusehen, welche besondere Zweckbindung dieses Datum in sich trägt. Um

die gesetzliche Zweckbindung feststellen zu können, müssen die Daten entsprechend gekennzeichnet werden, damit sich ihr Charakter im Laufe der Weiterverarbeitung nicht verliert.

Bei heimlichen Erhebungsmethoden der Polizei und des Verfassungsschutzes sind wegen der Schwere des Eingriffs vielfach besondere gesetzliche Zweckbindungen zu beachten. Den sachbearbeitenden Personen wird die Einhaltung datenschutzrechtlicher Bestimmungen durch die Kennzeichnung erleichtert, wenn nicht gar erst ermöglicht.
Im datenschutzgerechten Vollzug gesetzlicher Vorgaben, in denen die besondere Zweckbindung gesichert wird, darf die Kennzeichnung deshalb nicht fehlen.

3.4 Zusammenarbeit von Polizei und Verfassungsschutz zur Bekämpfung des islamistischen Terrorismus

Infolge der durch islamistische Terroristen verursachten Attentate in den USA und Spanien, denen zahlreiche Personen zum Opfer fielen, war es selbstverständliche Aufgabe aller Sicherheitsbehörden, Überlegungen anzustellen, ob eine verbesserte Zusammenarbeit der zuständigen Behörden zur Vermeidung, oder zumindest zur rascheren Aufklärung, dieser schwersten Straftaten beitragen könnte.

Die rechtlichen Möglichkeiten der Zusammenarbeit sind in den Polizei- und Verfassungsschutzgesetzen des Bundes und der Länder heute schon auf eindeutigen Grundlagen geregelt. Diese erlauben auch eine gemeinsame Datei mit den Daten solcher Personen, die sowohl nach Polizei- als auch nach Verfassungsschutzrecht gespeichert werden dürfen. Dabei ist zu beachten, dass der Polizei im Gegensatz zum Verfassungsschutz nicht die Aufgabe obliegt, extremistische Tätigkeiten im Vorfeld des konkreten Verdachts einer Straftat mit Geheimdienstmethoden zu beobachten. Dies ist die ausschließliche Domäne des Verfassungsschutzes. Überschneidungen ergeben sich allerdings bei Vorliegen eines terroristischen Sachverhalts, so dass insofern auf bereits vorhandene gesetzliche Grundlagen für eine Zusammenarbeit zurückgegriffen werden kann.

Von den Datenschutzbeauftragten des Bundes und der Länder wurde im Rahmen der 68. Konferenz in Saarbrücken auf die durch Aufnahme des islamistischen Extremismus ohne terroristischen Hintergrund entstehende Verwischung von Kompetenzen beider Behörden bei Führung einer gemeinsamen Datei hingewiesen. Die Beobachtungsaufgabe des Verfassungsschutzes mit weitgehenden Vorfeldbefugnissen, aber ohne die Befugnis im Einzelfall einschreiten zu dürfen, ist bislang streng getrennt vom Auftrag der Polizei zur vorbeugenden Bekämpfung und der Verfolgung und Ahndung von Straftaten einschließlich der dazugehörigen Exekutivbefugnisse. Dies ist ein Ausfluss des so genannten Trennungsgebotes, dessen Verfassungsrang zwar umstritten ist, das aber jedenfalls bewirkt, dass beide Behörden durch diese historisch begründete Trennung nicht in die Nähe der ehemaligen nationalsozialistischen Geheimen Staatspolizei (Gestapo) gerückt werden können.

In diesem Zusammenhang wird auch eine Verlagerung von Kompetenzen der Länder auf den Bund diskutiert. Übernimmt z.B. das Bundeskriminalamt oder das Bundesverfassungsschutzamt Kompetenzen, die noch teilweise bei den Ländern verbleiben, so weist dies nur dann eine Datenschutzrelevanz auf, wenn es nicht gelingt, Doppelzuständigkeiten zu vermeiden. Die Verantwortung für die Datenverarbeitung muss eindeutig sein, um transparent zu bleiben.
Der Staat sollte sich gerade angesichts des Terrorismus nicht dazu verleiten lassen, demokratische Prinzipien aufzugeben und damit Terroristen und ihren Zielsetzungen in die Hände zu spielen.

4 Justiz

4.1 Akustische Wohnraumüberwachung und verdeckte präventive Maßnahmen

Am 3. März 2004 hat das Bundesverfassungsgericht zwei für den Datenschutz bedeutsame Entscheidungen gefällt, die nicht nur den Bundes- sondern auch die Landesgesetzgeber zur Novellierung von Gesetzen veranlassen müssen.

In beiden Fällen handelte es sich um Verfassungsbeschwerden von Personen, die sich in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt sahen.

Das Bundesverfassungsgericht hat in seinem Urteil zur akustischen Wohnraumüberwachung (1 BvR 2378/98; 1 BvR 1084/99) in erster Linie hervorgehoben, dass es einen absoluten Kernbereich privater Lebensgestaltung gibt, in den der Staat nach dem Grundsatz der Unantastbarkeit der Menschenwürde gem. Art. 1 Abs. 1 Grundgesetz nicht eindringen darf.

Wenn es um die Konsequenz dieses Prinzips nach der Entscheidung des Bundesverfassungsgerichtes geht, kann es keinen Unterschied machen, in welcher Rechtsmaterie sich der Gesetzgeber bewegt, die absolute staatliche Garantie der Wahrung des Kernbereichs privater Lebensgestaltung ist in der Regelung jeglicher Rechtsmaterie sicherzustellen.

Die Bundesregierung hat zur Umsetzung des Urteils den Entwurf einer Änderung der Strafprozessordnung vorgelegt, der allerdings erst im zweiten Anlauf in etwa den Vorgaben der bundesverfassungsgerichtlichen Entscheidung entsprach. Einzelheiten werden in der parlamentarischen Diskussion noch zu erörtern sein.

Der Landesgesetzgeber hat vor allen Dingen die Gesetze zu novellieren, in denen Verfahren zur verdeckten Datenverarbeitung geregelt sind, wie z.B. im Polizei- und Verfassungsrecht.

Dazu hat das Bundesverfassungsgericht in seiner weiteren Entscheidung vom 3. März 2004 (1 BvF 3/92), die zu den im Außenwirtschaftsgesetz geregelten präventiven Befugnissen des Zollkriminalamtes ergangen ist, ausdrücklich die Beachtung der Grundsätze in seiner Entscheidung zur akustischen Wohnraumüberwachung angemahnt. Zusätzlich hat das Bundesverfassungsgericht bei der im Außenwirtschaftsgesetz geregelten präventiven Telefonüberwachung die fehlende Normenklarheit wegen einer zu großen Verschachtelung von in Bezug genommenen Tatbeständen („Kaskaden“) gerügt. Das Bestimmtheitsgebot habe zu gewährleisten, dass „die möglichen Anlässe einer Überwachungsmaßnahme nicht uferlos zu werden drohen“.

Dem Innenministerium habe ich die Zusammenfassung der Entscheidungsgrundsätze, die auch dem Vorsitzenden der Innenministerkonferenz über den Bundesbeauftragten für den Datenschutz übersandt wurde, zur Kenntnis übermittelt. Dazu zählen insbesondere:

- Schutz der Kommunikationsinhalte, insbesondere bei Gesprächen mit Familienangehörigen oder Vertrauten sowie mit Berufsgeheimnisträgern;
- Überprüfung der Straftatenkataloge, insbesondere bei Eingriffsbefugnissen, bei denen der Gesetzgeber ein bestimmtes Gewicht der zu verhütenden Tat voraussetzt;
- Eingrenzung der Eingriffsermächtigung bei präventiver Überwachung, indem an Tatsachen angeknüpft wird, die einen erfahrungsgemäß hinreichend sicheren Schluss auf die Tatsachenbasis und auf den Grad der Wahrscheinlichkeit der geplanten Straftat zulassen;
- eindeutige Regelung der Löschung und ggf. Sperrung sowie Verpflichtung zur Löschung bei rechtswidriger Erhebung im Kernbereich privater Lebensgestaltung;
- Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten sowie eine Kennzeichnungspflicht zur Sicherstellung der Zweckbindung;
- Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen, von der allenfalls abzusehen ist, wenn die Identität der Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden könnte oder der Benachrichtigung überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. In diesem Zusam-

menhang ist sicherzustellen, dass gesetzliche Löschungsverpflichtungen den Rechtsschutz in den Fällen nicht unterlaufen, in denen von Betroffenen eine gerichtliche Kontrolle staatlicher Datenverarbeitungsvorgänge angestrebt wird;

- gesetzliche Festlegung der Zeitabstände für eine Benachrichtigung und verfahrensrechtliche Sicherung der Einhaltung der gebotenen Benachrichtigungspflicht durch unabhängige Gremien, die die Fälle prüfen, in denen die Benachrichtigung aus Geheimhaltungsgründen nicht erfolgt.

Bislang ist glücklicherweise die präventive Telefonüberwachung im saarländischen Polizeigesetz nicht zugelassen. Ich würde es sehr begrüßen, wenn von dieser Maßnahme, die in der Vergangenheit offensichtlich nicht benötigt wurde, auch weiterhin Abstand genommen würde. Die in der Strafprozessordnung geregelte (repressive) Telefonüberwachung lässt in Fällen drohender Straftaten i.S.d. § 138 Strafgesetzbuch und entsprechendem Tatverdacht die Befugnisse der Polizei als ausreichend erscheinen.

Aufgrund der Heimlichkeit aller verdeckten Maßnahmen und der demnach starken Eingriffsintensität in das Recht auf informationelle Selbstbestimmung hat der Gesetzgeber sorgfältig zu prüfen, welchen Schutz er den Betroffenen durch ein rechtsstaatliches Verfahren der Datengewinnung und Datennutzung bieten muss.

4.2 Aufzeichnen von Verteidigergesprächen bei der Telefonüberwachung

Durch die Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zur akustischen Wohnraumüberwachung und zu den präventiven heimlichen Maßnahmen der Sicherheitsbehörden ist auch eine weitere Thematik betroffen, die im Berichtszeitraum Aufsehen erregt hat.

Presseberichten zufolge hat die saarländische Polizei in einem Einzelfall bei einer strafprozessualen Telefonüberwachung ein Gespräch des Beschuldigten mit seinem Verteidiger nach der stets stattfindenden elektronischen Aufzeichnung ausgewertet,

verschriftet und der staatsanwaltschaftlichen Ermittlungsakte beigefügt. Nach meinen Prüfungserfahrungen zu Telefonüberwachungsmaßnahmen konnte ich nicht bestätigen, dass es sich dabei um eine generelle Verfahrensweise der Polizei gehandelt hat.

Zunächst ist davon auszugehen, dass Polizeibeamte im strafprozessualen Verfahren Ermittlungspersonen der Staatsanwaltschaft sind, so dass die Staatsanwaltschaft Herrin des Verfahrens ist und daher jede Maßnahme der Polizei rechtlich ausschließlich der Staatsanwaltschaft zuzuordnen ist. Das Gebot der Strafprozessordnung (StPO), dem Beschuldigten im Regelfall (unüberwachten) schriftlichen und mündlichen Verkehr mit dem Verteidiger zu gestatten (§ 148 Abs. 1 StPO), richtet sich daher in erster Linie an die Staatsanwaltschaft, die sich der Polizei zur Ausführung von Überwachungsmaßnahmen bedient. Demgemäß hat die Staatsanwaltschaft durch Weisungen an die Polizei ein Verfahren zu gewährleisten, das den Vorgaben des Bundesverfassungsgerichts entspricht.

Strafverteidiger gehören zu dem Personenkreis, zu dem ein besonderes Vertrauensverhältnis besteht; Überwachungsmaßnahmen zu diesen Personen dürfen nur dann ergriffen werden, wenn konkrete Anhaltspunkte dafür bestehen, dass die Gesprächsinhalte zwischen dem Beschuldigten und seinem Verteidiger keinen absoluten Schutz erfordern, so bei einer Tatbeteiligung der das Gespräch führenden Person. Solche Anhaltspunkte müssen aber schon vor der Anordnung zur Überwachung bestehen und dürfen nicht erst durch die Überwachung begründet werden (s. a. Pressemitteilung Nr. 22/2004 vom 3.3.2004 des Bundesverfassungsgerichts zu 1 BvR 2378/98 und 1 BvR 1084/99).
Das würde zunächst bedeuten, dass im Regelfall die Überwachung sofort unterbrochen werden muss, wenn ein Gespräch als Verteidigergespräch zu qualifizieren ist. Will man der Polizei die Erschwernis des ständigen Mithörens nicht auferlegen, da die moderne Technik ein selbständiges Aufzeichnen der Gespräche bietet, so ist spätestens beim Abhören der Aufzeichnungen das Mithören zu unterbrechen. Keinesfalls darf ein solches Gespräch auch noch verschriftet und zur Akte genommen werden.

An dieser Stelle sei daran erinnert, welche Kriterien für den Einsatz der Technik zu gelten haben. Kann die Technik einen datenschutzgerechten Einsatz nicht gewährleisten, so darf sie nicht eingesetzt werden. Das bedeutet im vorliegenden Fall, eine technische Aufzeichnung dürfte eigentlich nicht stattfinden. Nach dem gegenwärtigen Stand der Technik kann diese das Herausfiltern eindeutiger Verteidigergespräche nicht leisten, da nur mit Hilfe menschlicher Bewertungen erkannt werden kann, um welche Art von Gespräch es sich handelt.

Aus der Sicht des Datenschutzes hat hier eine Korrektur dieses technischen „Mangels“ stattzufinden, d.h. die (technisch) aufgezeichneten Verteidigergespräche sind, sobald sie von der abhörenden Person als solche qualifiziert werden, unverzüglich zu löschen.

Die Staatsanwaltschaft hat die Polizei zur Beachtung der bundesverfassungsgerichtlichen Vorgaben dahingehend anzuweisen. Sie darf nicht zulassen, dass Verteidigergespräche verschriftet, auch noch zu den Akten gereicht und dort bis zum Ende des Verfahrens aufbewahrt werden.

Eine Überarbeitung der Richtlinie zur Telekommunikationsüberwachung wurde mir kürzlich im Entwurf vorgelegt. Sie bedarf allerdings noch der eindeutigen Präzisierung hinsichtlich der grundsätzlichen Unzulässigkeit des Abhörens von Verteidigergesprächen.

4.3 Datenschutz im Strafvollzug

4.3.1 Verteilung von monatlichen Verdienstabrechnungen

Ein Strafgefangener der JVA Saarbrücken hat sich darüber beschwert, dass die monatlichen Verdienstabrechnungen, die neben Namen, Geburtstag, Geburtsort auch Daten über die finanzielle Situation des Gefangenen wie z.B. Rücklagen und Sparguthaben enthalten, von der Zahlstelle offen und für jeden zugänglich verteilt werden.

Die offene Weitergabe von Verdienstabrechnungen war bereits durch die Rechtsprechung in anderen Bundesländern in unterschiedlicher Weise beurteilt worden. So hat die Strafvollstreckungskammer des Landgerichts Trier entschieden, Kontoauszüge und Einzahlungsbelege der Strafgefangenen seien in verschlossenen Umschlägen zu verteilen (57 StVK 645/02).
Dieser Beschluss wurde jedoch vom Oberlandesgericht Koblenz aufgehoben (1 Ws 303/03). Zwar wurde anerkannt, dass es sich bei den Kontoauszügen und Einzahlungsbelegen um personenbezogene Daten handelt, die grundsätzlich dem Schutz des § 183 StVollzG unterliegen und dass ein größtmöglicher Schutz nur dadurch gewährleistet werden kann, indem die Ausdrucke in Umschläge gesteckt, diese verschlossen und in diesem Zustand an die Gefangenen ausgehändigt werden.

Das Oberlandesgericht Koblenz sah ein Versäumnis der Strafvollstreckungskammer darin, dass eine Abwägung der Interessen des Strafgefangenen gegen das berechtigte Interesse der Justizvollzugsanstalt, mit Rücksicht auf deren personelle Ressourcen von übermäßigem Personal- und Organisationsaufwand verschont zu bleiben, nicht vorgenommen wurde. Der auf die JVA zukommende personelle und organisatorische Aufwand stehe zu der angestrebten Schutzwirkung in keinem angemessenen Verhältnis. Bei den Kontoauszügen handele es sich darüber hinaus um nicht besonders schützenswerte Daten. (Ähnlich urteilte das Hanseatische Oberlandesgericht, 3 Vollz (Ws) 31/03.)

Aus Sicht des Datenschutzes ist diese Beurteilung unbefriedigend, da in § 183 Abs. 2 StVollzG geregelt ist, dass Akten und Dateien mit personenbezogenen Daten durch die erforderlichen technischen und organisatorischen Maßnahmen gegen unbefugten Zugang und unbefugten Gebrauch zu schützen sind. Die Einschätzung, Kontendaten seien nicht besonders schützenswert ist sehr fragwürdig, da außerhalb des Justizvollzugs dieser Bereich zumindest dem vertraglich vereinbarten Bankgeheimnis unterliegt.

Aufgrund der eindeutigen, aber unbefriedigenden Rechtsprechung konnte eine datenschutzgerechtere Verfahrensweise nicht erzielt werden.

4.3.2 Namensschilder an Haftraumtüren

Weitere Eingaben hatten zum Inhalt, dass die JVA Saarbrücken neuerdings an den Haftraumtüren Namensschilder mit Vor- und Zunamen der Insassen angebracht hat. Dies führt dazu, dass nicht nur Anstaltspersonal und Mithäftlinge, sondern auch Besucher Informationen darüber erhalten, wer sich dort befindet. Die Petenten halten diese Maßnahme für überflüssig, fühlen sich bloß gestellt und sehen ihr Recht auf informationelle Selbstbestimmung verletzt.

Die JVA Saarbrücken hat in ihrer Stellungnahme mehrere Faktoren aufgeführt, die zu der Maßnahme geführt haben:
Durch Überbelegung werden auch Funktionsräume in erster Linie für Neuzugänge als Hafträume genutzt. Bei Freiwerden originärer Hafträume werden Umzüge veranlasst, worunter die Kontinuität der Belegung in den Abteilungen und letztlich die Überschaubarkeit leidet.
Die Überbelegung führt zu einem Personalmehrbedarf, der durch Neueinstellungen ausgeglichen wird. Das neue Personal durchläuft während der Ausbildung unterschiedliche Abteilungen und ist infolgedessen mit den Namen der Insassen nicht vertraut.
Weiterhin sind in zunehmendem Maße Getrennthaltungen zu beachten. Um dies vor dem Hintergrund der Überbelegung und des häufigeren Personalwechsels organisatorisch bewerkstelligen zu können, schafft auch hier die Beschriftung der Haftraumtüren eine wesentliche Erleichterung.

In einer ähnlichen Konstellation ist die Rechtsprechung des Bundesverfassungsgerichts davon ausgegangen, dass, sofern die problemlose Abgrenzung von Raumzuteilungsverhältnissen und das geordnete Zusammenleben in einer Anstalt es erfordern, die Beschriftung an Haftraumtüren durchaus zulässig und verfassungsrechtlich zu rechtfertigen ist (2 BvR 2650/94).

Ich habe allerdings angeregt, die Beschriftungen für den vorübergehenden Zeitraum abzukleben, wenn beispielsweise Besuchergruppen durch eine Abteilung geführt

werden. Die Erforderlichkeit der Kenntnisnahme von Insassennamen ist meines Erachtens bei solchen und ähnlichen Anlässen nicht gegeben.
Die Anstaltsleitung ist wegen der damit verbundenen unverhältnismäßig hohen Belastung für das Anstaltspersonal unter Berufung auf eine gleich lautende Rechtsprechung unserer Anregung nicht gefolgt.

Durch die Einschränkung der Zulassung von Besuchergruppen, deren Auswahl und Verschwiegenheitspflichten soll jedoch dem Datenschutz der betroffenen Inhaftierten zukünftig besser Rechnung getragen werden.

4.4 Erweiterung der DNA-Analyse

Nach (fast) jeder spektakulären Straftat werden aus dem politischen Raum Forderungen zur Erweiterung der DNA-Analyse in Strafverfahren laut. Im Jahre 2001 hatte sich dies bis zu dem Ansinnen der anlasslosen DNA-Analyse für alle Männer der Bundesrepublik Deutschland gesteigert (vgl. 19. TB, TZ 4.4). Die Umsetzung einer solchen Forderung wäre eindeutig verfassungswidrig. Aber auch wenn der Anlass zu einem Strafverfahren vorliegt, so setzt letztendlich der Verhältnismäßigkeitsgrundsatz Grenzen bei der Untersuchung von genetischen Strukturen eines Menschen, weil damit ein tiefer Eingriff in sein Recht auf informationelle Selbstbestimmung verbunden ist.

Wie die Erfahrung zeigt, werden beim Aufbau und der Existenz von Datenbanken stets Begehrlichkeiten unterschiedlicher Stellen wach, so dass die gesetzlich einmal festgelegte Zweckbestimmung der Daten auf die Dauer vielfach nicht mehr für wünschenswert gehalten wird. Dies könnte beispielsweise bedeuten, dass Arbeitgeber und Versicherungen an diesen Datenmengen für die Verfolgung ihrer Ziele großes Interesse zeigen. Um insoweit klare Vorgaben zu schaffen, ist es notwendig, die Planungen zu einem Gendiagnostikgesetz des Bundes zu einem zufrieden stellenden Abschluss zu bringen.

Unabhängig davon kann die Wissenschaft bereits heute darlegen, um wie viel größer der Erkenntnisgewinn durch die DNA-Analyse im Gegensatz zum Fingerabdruck ei-

nes Menschen ist, so dass beide Methoden der erkennungsdienstlichen Maßnahmen nicht miteinander gleichgesetzt werden können. So können aus der DNA trotz der vorgeschriebenen Untersuchung des bloßen „nicht-codierenden“ Teils neben dem Geschlecht eines Menschen bereits Altersabschätzungen, Zuordnungen zu bestimmten Ethnien und auch möglicherweise einige Krankheiten abgeleitet werden.

Derartig tiefe Einblicke in die genetischen Anlagen einer Person erfordern im Strafverfahren das Beibehalten einer Straftat von erheblicher Bedeutung und den Richtervorbehalt als Voraussetzung für die Anordnung und Durchführung einer DNA-Analyse.
Die Datenschutzbeauftragten des Bundes und der Länder haben daher in einer erneuten Entschließung (Anlage 15.10) darüber hinaus hervorgehoben, wie weitgehend die Konsequenzen für Nichttäterinnen und Nichttäter bis hin zur Umkehr der Beweislast für ihre Unschuld sein können.

4.5 Justizakten im Papiercontainer

Von privater Seite wurden mir 6 Aktenhefter der Staatsanwaltschaft Saarbrücken übergeben, die mühelos aus einem Papiercontainer zu entnehmen waren, als der Finder für seinen eigenen Papierabfall Platz schaffen wollte. Es handelte sich dabei um Kopien von Auszügen aus Originalakten. Nachnamen waren teilweise geschwärzt, teilweise im Klartext vorhanden. Geburtsdaten, Adressen und andere personenbezogene Daten waren nicht geschwärzt.

Die Vorgänge enthielten den Gang des jeweiligen Verfahrens darstellende Schriftstücke bis zum entsprechenden Urteil. Ihnen lagen Sachverhalte aus den Jahren 1986-1991 zu Grunde.

Es ist immer wieder erstaunlich, wie sorglos selbst Amtspersonen mit den ihnen zur Verfügung gestellten amtlichen Arbeitsmitteln umgehen, in denen – gerade in Strafverfahren – sehr sensible personenbezogene Daten enthalten sind. Offensichtlich fehlten auch grundlegende Kenntnisse zur datenschutzgerechten Papierentsorgung, trotz entsprechender Dienstanweisungen für alle öffentlichen Stellen.

Geradezu besorgniserregend war auch die Tatsache, dass die Aktenkopien wohl zu Ausbildungszwecken zur Verfügung gestellt wurden. Man kann sich leicht vorstellen, welche Bedeutung dem Aspekt des Datenschutzes in dieser Ausbildung zukam, ungeachtet dessen, ob der Ausbilder oder die Ausbilderin diese Aktenkopien derart unsachgemäß selbst „entsorgt“ hatten oder gar Auszubildende mit dieser Aufgabe betraut worden sind.

Dem Leitenden Oberstaatsanwalt, der um die Aufklärung der Angelegenheit bemüht war, die verantwortliche Person jedoch nicht ermitteln konnte, war im Hinblick auf den in Betracht zu ziehenden Personenkreis insofern zuzustimmen, als es sich hierbei nicht zwingend um Bedienstete der Staatsanwaltschaft handeln musste. In die Ausbildung sind auch Bedienstete der Gerichte einbezogen.

Um solchen Missständen soweit wie möglich entgegen zu wirken, hat der Leitende Oberstaatsanwalt daher nochmals auch die zuständigen Gerichte darauf hingewiesen, dass zu Ausbildungszwecken angelegte Auszüge aus Originalakten der Verwaltungsgeschäftsstelle der Staatsanwaltschaft zur Vernichtung zu übergeben sind.
Solche Datenschutzverstöße sollten nach jahrzehntelanger Bewusstseinsbildung für die Persönlichkeitsrechte Betroffener wirklich nicht mehr vorkommen.

4.6 Online-Abrufverfahren beim automatisierten Grundbuch

Im Jahr 2002 wurde das „elektronische Grundbuch“ eingerichtet, welches für das Saarland durch das Saarländische Grundbuchamt beim Amtsgericht Saarbrücken geführt wird. Wesentlicher Bestandteil des elektronischen Grundbuchs ist dabei das automatisierte Abrufverfahren, das es vorbehaltlich der Genehmigung durch die Landesjustizverwaltung den Gerichten, Behörden, Notaren, öffentlich bestellten Vermessungsingenieuren und anderen in § 133 Grundbuchordnung genannten Personen und Einrichtungen erlaubt „online“ auf Daten des Grundbuchs Zugriff zu nehmen. Eine Voraussetzung für die Einrichtung des Online-Abrufs ist die Protokollierung der Abrufe um deren Zulässigkeit überprüfen zu können.

Anhand zufällig ausgewählter Protokolle wurde bei der überprüften Kommune festgestellt, dass die Protokollierung mangelhaft war. Entgegen den Bestimmungen des § 83 Grundbuchverfügung (GBV) war das Geschäfts- oder Aktenzeichen der abrufenden Stelle nicht angegeben. In den einzelnen Fällen konnte daher das berechtigte Interesse für den Abruf teilweise nur aufgrund unvollständiger, handschriftlicher Aufzeichnungen bzw. dem Erinnerungsvermögen des Sachbearbeiters nachvollzogen werden.

Ich habe die Justizverwaltung gebeten, die beteiligten öffentlichen Stellen darauf hinzuweisen, dass den Voraussetzungen des § 83 GBV in der Protokollierung entsprochen werden muss. In diesem Zusammenhang bat ich um Mitteilung, welche Stelle die Stichprobenkontrollen nach § 83 Abs. 1 Satz 3 GBV durchführt. Eine Antwort auf diese Frage steht noch aus.

Strittig ist überdies die Frage der regionalen Beschränkung der Abrufmöglichkeiten für die Kommunen. Die Angemessenheit eines online-Abrufverfahrens hat sich aus der Sicht des Datenschutzes am verfassungsrechtlichen Verhältnismäßigkeitsprinzip zu orientieren. Somit darf über den tatsächlichen Bedarf an vielzähligen oder eilbedürftigen Übermittlungen zu personenbezogenen Daten der Einwohner/innen bzw. zu Grundstücken einer Gemeinde hinaus nicht der Datenbestand eines ganzen Bundeslandes oder gar der gesamten Bundesrepublik zum Abruf bereit gehalten werden.

Die Angemessenheit, die im Genehmigungsverfahren zu überprüfen ist, kann sich lediglich in Relation auf den Datenbestand ergeben, der konkret einen territorialen Bezug zur Gemeinde aufweist. Darüber hinaus gehende Datenübermittlungen, die durchaus zulässig sein können, vermögen aufgrund der Seltenheit oder fehlender gehäufter Eilbedürftigkeit ein online-Verfahren nicht zu rechtfertigen.

Leider bietet das technische Verfahren nicht die notwendigen aus der Verfassung herzuleitenden Beschränkungsmöglichkeiten. Darum sollte sich die Justizverwaltung aber weiterhin bemühen, auch wenn das Verfahren sich in dieser Ausgestaltung bereits in zahlreichen Bundesländern im Einsatz befindet.

4.7 Telefonüberwachung

Der Aufforderung der Datenschutzbeauftragen des Bundes und der Länder (Anlage 15.6) auch weiterhin die Transparenz im Hinblick auf die Anzahl der Telefonüberwachungen mit Hilfe einer Unternehmensstatistik zu gewährleisten, ist der Gesetzgeber erfreulicherweise im neuen Telekommunikationsgesetz (§ 110 Abs. 8 TKG) nachgekommen.
Die von den Landesjustizverwaltungen parallel erstellten Statistiken erfassen lediglich das jeweilige Strafverfahren, nicht jedoch die einzelnen überwachten Anschlüsse und sind daher nicht aussagekräftig genug.

Wie stark die Anzahl der Telefonüberwachungen in dem Zeitraum von 1996 – 2001 angestiegen ist, hat auch ein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten des Max-Planck-Instituts belegt, wonach allein die Ermittlungsverfahren mit TKÜ-Anordnungen einen Zuwachs von 80 % in diesen 5 Jahren zu verzeichnen hatten.

Aber nicht nur der zahlenmäßige Anstieg, auch die übrigen Defizite in den gesetzlichen Vorgaben und dem Vollzug der Telefonüberwachungen sind besorgniserregend. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung (Anlage 15.13) verdeutlicht, wie die Situation durch den Gesetzgeber aber auch im Vollzug verbessert werden sollte.

Ohne Zweifel erleichtert die Telefonüberwachung die polizeiliche und staatsanwaltliche Ermittlungsarbeit erheblich. Sie darf als schwerwiegender Eingriff in das Telekommunikationsgeheimnis und Grundrecht nach Art. 10 GG jedoch nicht über die Jahre hinweg und mit fortschreitender Technisierung zur Standardmaßnahme im Ermittlungsverfahren ausarten.

Die Telefonüberwachung im Strafverfahren zählt zu den heimlichen Ermittlungsmethoden, die nach den Entscheidungen des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung in der StPO und präventiven Telefonüberwachung im

Außenwirtschaftsgesetz (vgl. TZ 4.1) einer Generalüberholung in den jeweiligen Rechtsnormen bedarf.

4.8 Neuregelung bei Kirchenaustritten

Es gehört zur guten jahrzehntelangen Tradition, den Landesbeauftragten für Datenschutz in Gesetzgebungsverfahren, in denen es um die Regelung der Verarbeitung personenbezogener Daten geht, aber auch bei der Abfassung von einschlägigen Rechtsverordnungen zu beteiligen. Für Verwaltungsvorschriften ist die Anhörung des Landesbeauftragten für Datenschutz im Saarländischen Datenschutzgesetz ausdrücklich festgehalten (§ 7 Abs. 1 Satz 2).

Umso überraschender war für mich die Feststellung, dass sich die Rechtslage bei der Erklärung von Kirchenaustritten im Vergleich zu meiner Darstellung im 19. TB (TZ 4.5) und dem damals geltenden Recht zwischenzeitlich geändert hatte.

Die Änderung ist zurückzuführen auf Art. 18 des Deregulierungsgesetzes (Amtsbl. 2004, 1037), wonach – statt des bisher zuständigen Amtsgerichts – nunmehr die Wohnsitzgemeinde des Betroffenen für eine Kirchenaustrittserklärung zuständig ist. Die Mitteilung des Amtsgerichts an das Standesamt ist damit vom Wortlaut her zunächst entfallen. Innerhalb der Kommunalverwaltung sollten aus der Sicht des Datenschutzes nunmehr ausschließlich die Meldebehörden für Kirchenaustrittserklärungen als ohnehin zuständige Verwaltungsstelle bestimmt werden, weil sie dieses Datum schon für die Ausstellung von Lohnsteuerkarten benötigen.

Wie in meinem 19. TB bereits ausgeführt, reichen die im Personenstandsrecht geregelten Anlässe zur Datenerhebung durch die Standesämter zur Erreichung staatlicher Ziele aus.

Ich hätte erwartet, in dieser datenschutzrelevanten Angelegenheit beteiligt zu werden, aber weder der Entwurf des Deregulierungsgesetzes noch die entsprechende Aufhebung der Regelung in der Anordnung über die Mitteilung in Zivilsachen wurden mir vorgelegt. Dem äußeren Anschein nach hat sich die Situation für den Betroffenen

zwar verbessert, da eine dritte Stelle (Amtsgericht) in die Kenntnis eines Kirchenaustritts nicht einbezogen wird.

Ob der Gang zur Wohnsitzgemeinde für denjenigen, der aus der Kirche austreten möchte, gerade in kleineren Kommunen weniger heikel ist als der Gang zu dem doch gewöhnlich anonymeren Amtsgericht möchte ich allerdings bezweifeln.

5 Polizei

5.1 Änderungen im Polizeigesetz

Bei Gelegenheit der Einfügung einer Bestimmung zur Bekämpfung der häuslichen Gewalt durch Platzverweisung, Wohnungsverweisung und Aufenthaltsverbot wurden im Jahre 2004 auch Eingriffsschwellen für die Datenverarbeitung der Polizei herabgesenkt. Im Jahr zuvor hatte man das Gesetz zur Durchführung des Terrorismusbekämpfungsgesetzes zum Anlass genommen, die Voraussetzungen für die Durchführung einer Rasterfahndung aus der Sicht des Datenschutzes zu verschlechtern. Nunmehr soll lediglich eine Gefahr und nicht mehr eine „gegenwärtige" Gefahr die Durchführung einer Rasterfahndung rechtfertigen. Auch müssen nicht mehr „tatsächliche Anhaltspunkte die Annahme rechtfertigen", dass die Rasterfahndung zur Abwehr der Gefahr erforderlich ist.

Das nicht nur datenschutzrechtlich, sondern auch von seiner Effizienz her sehr umstrittene Instrument der Rasterfahndung, das die Einbeziehung massenhaft Unschuldiger mit sich bringt, dürfte meines Erachtens nicht unter derart erleichterten Bedingungen einsetzbar sein. Dies habe ich im Gesetzgebungsverfahren – leider vergeblich – mehrfach betont.

Dennoch hat sich im eingangs erwähnten Gesetz der Trend zur schrittweisen datenschutzrechtlichen Verschlechterung der Voraussetzungen für ein polizeiliches Einschreiten fortgesetzt. Nunmehr darf die Polizei sich auf Erfahrungen aus der Vergangenheit bei der Datenverarbeitung verlassen, was durch die Einfügung des Wortes „erfahrungsgemäß" legalisiert wurde (§ 30 Abs. 3 Satz 1 SPolG), womit der Einzelfall durchaus aus dem Blickfeld geraten kann.

Sozusagen im Fortsetzungszusammenhang mit dem Wegfall tatsächlicher Anhaltspunkte bei der Rasterfahndung wurden in der allgemeinen Bestimmung zur Datenspeicherung, -veränderung und –nutzung auch hier die Attribute „tatsächliche" vor dem Wort „Anhaltspunkte" gestrichen. Diese Änderung halte ich auch nicht deswe-

gen für weniger gravierend, weil bei der vorbeugenden Straftatenbekämpfung nach dieser Bestimmung Verbrechen oder Straftaten von Organisationen oder Banden in Aussicht stehen müssen, die gewerbs- oder gewohnheitsmäßig begangen sein könnten. Gerade bei solchen Delikten dürfte die Polizei den Boden der Tatsachen nicht verlassen dürfen.

Es ist leider festzustellen, dass die Polizei durch solche schrittweise zugebilligten Befugnisse mehr und mehr in das sogen. Vorfeld einer polizeilichen Gefahr oder auch vorbeugender Straftatenbekämpfung gerät und sich von ihrer ursprünglichen tatsachenorientierten Aufgabenstellung immer weiter entfernt.

Auch das Bundesverfassungsgericht (1 BvF 3/92) hat in seiner Entscheidung zur präventiven Telekommunikationsüberwachung durch das Zollkriminalamt vom 3.3.2004 betont, dass Eingriffsermächtigungen an Tatsachen anknüpfen müssen, die einen hinreichend sicheren Schluss auf den Grad der Wahrscheinlichkeit geplanter Straftaten zulassen.

Als Konsequenz aus dieser verfassungsgerichtlichen Vorgabe ist die Forderung abzuleiten, zum ursprünglichen Wortlaut der Bestimmungen spätestens bei der notwendigen Änderung des Polizeigesetzes aus Anlass der bundesverfassungsgerichtlichen Entscheidungen vom 3.3.2004 zurückzukehren (s. TZ 4.1).

5.2 Automatische Kfz-Kennzeichenerfassung durch die Polizei

Das Saarland gehörte zu den Bundesländern, die nach Presseverlautbarungen die anlassfreie automatische Kfz-Kennzeichenerfassung nicht einführen wollten.

Planungen in anderen Ländern haben die Datenschutzbeauftragten des Bundes und der Länder dazu veranlasst, auf die damit verbundene Gefahr einer neuen verstärkten Überwachungsinfrastruktur hinzuweisen (Anlage 15.17).

An dieser Stelle wollte ich ursprünglich alle Verantwortlichen dazu ermutigen, bei ihrer ablehnenden Haltung zu bleiben, einem etwaigen Anpassungsdruck an andere

Bundesländer standzuhalten und dadurch auch nicht Gefahr zu laufen, verfassungswidrige Normen des Polizeirechts zu schaffen.

Zwischenzeitlich habe ich erfahren, dass der automatische Kfz-Datenabgleich auch im Saarland stattfinden soll.
Inwieweit er durch die technische Ausgestaltung als noch verhältnismäßig anzusehen ist, wird im Einzelnen noch zu prüfen sein.

5.3 Erforderlichkeit der Erhebung des Geburtsdatums

Bagatellen können mitunter zur Einleitung eines Bußgeldverfahrens führen. Dies musste ein Bürger erfahren, dessen Nachtruhe durch anhaltenden nachbarlichen Lärm gestört wurde und der sich deshalb Hilfe suchend telefonisch an die Polizei gewandt hatte. Er wurde nach Vorname, Name, Straße und Wohnort befragt, worüber er bereitwillig Auskunft erteilte. Die zusätzliche Frage nach seinem Geburtsdatum schien ihm jedoch zu weitgehend und in diesem Zusammenhang nicht von Bedeutung, weshalb er sie nicht beantwortete.

Als Reaktion auf sein Verhalten erhielt er einen Bußgeldbescheid, der inhaltlich mit dem Vorwurf einer Ordnungswidrigkeit nach § 111 Ordnungswidrigkeitengesetz begründet wurde. Daraufhin hat der Bürger sich mit der Frage, ob er wegen jeder Kleinigkeit solche Fragen beantworten müsse, an mich gewandt.

Die zur Begründung angeführte Bestimmung sieht für den Fall einer unrichtigen Angabe oder der Verweigerung verschiedener Daten auf Befragung durch einen Amtsträger die Feststellung und Ahndung einer Ordnungswidrigkeit vor. Bei den Daten handelt es sich um Vor-, Familien- oder Geburtsnamen, den Ort oder Tag der Geburt, den Familienstand, den Beruf, den Wohnort, die Wohnung oder die Staatsangehörigkeit.

Zwar ist im gesetzlichen Tatbestand der Ordnungswidrigkeit auch der Tag der Geburt aufgeführt. Nicht beachtet wurde im konkreten Fall jedoch die Voraussetzung der Erforderlichkeit der Erhebung eines personenbezogenen Datums für die jeweilige

amtliche Tätigkeit. Auch wenn das Gesetz die Zulässigkeit der Erhebung eines Datums festlegt, ist dennoch stets zu prüfen, ob dieses Datum für die Aufgabenerledigung einer Behörde tatsächlich erforderlich ist. Ist dies zu verneinen, kann dem Bürger nicht eine Ordnungswidrigkeit vorgehalten werden, sondern vielmehr dem Amtsträger eine unzulässige Datenerhebung.

Aus der Sicht des Datenschutzes wird häufig angeregt, die Erforderlichkeit einer Datenerhebung sowie aller weiteren Schritte der Datenverarbeitung nochmals gesetzlich festzuschreiben, obwohl die Erforderlichkeit ein allgemein gültiges Verfassungsprinzip staatlichen Handelns darstellt und daher die Wiederholung als überflüssig angesehen werden kann.

Wie der vorliegende Fall belegt, geraten Verfassungsprinzipien, die nicht im Gesetz wiederholt werden, schneller in Vergessenheit.

Wegen der (berechtigten) Weigerung des Bürgers, sein Geburtsdatum anzugeben, sollte allerdings ein Ordnungswidrigkeitenverfahren nicht eingeleitet werden. Der Bußgeldstelle habe ich daher empfohlen, das Verfahren einzustellen.

5.4 Speicherung von Daten ohne kennzeichnende Zusätze

Ein Petent hatte mich um Überprüfung seiner bei der Polizei des Saarlandes gespeicherten Daten gebeten.

Nach Auskunft des Landeskriminalamtes waren unter anderem Speicherungen von Straftaten aus dem Zeitraum 1980-1989 vorhanden. Ob diese Straftaten dem Petenten zugeordnet werden durften, war nicht zu klären, da weder ein Aktenzeichen noch der Ausgang eines Verfahrens bei der Staatsanwaltschaft und der Polizei zu ermitteln waren. Aktenunterlagen zu den Vorgängen waren ebenfalls nicht mehr vorhanden. Im damaligen Zeitraum bestand auch noch keine Verpflichtung der Staatsanwaltschaft zur Unterrichtung der Polizei über den Ausgang des Verfahrens (§ 482 Abs. 2 StPO).

Ich habe das Landeskriminalamt um Löschung dieser gespeicherten Daten gebeten und darüber hinaus auf die grundsätzliche Bedeutung der Angelegenheit hingewiesen.

Aus datenschutzrechtlicher Sicht müssen belastende Speicherungen von Daten über Straftaten und Zuordnungen zu einer Person Mindestvoraussetzungen erfüllen, die dann nicht vorliegen, wenn lediglich ein Straftatenverdacht ohne staatsanwaltliches Aktenzeichen und – nach Erledigung – ohne Benennung des Verfahrensausgangs (Verurteilung, Freispruch, Einstellung) gespeichert wurde.

In diesen Fällen ist es nicht im Geringsten nachzuvollziehen, ob die gesetzlichen Voraussetzungen des § 30 Abs. 2 Saarländisches Polizeigesetz (SPolG) eingehalten wurden. Nach dieser Bestimmung ist es der Polizei nur erlaubt, eine sogenannte Verdächtigendatei zu führen, „wenn dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, weil wegen der Art, Ausführung oder Schwere der Tat oder der Persönlichkeit der oder des Betroffenen die Gefahr der Wiederholung besteht."

Wenn nicht einmal ansatzweise belegt werden kann, ob die Staatsanwaltschaft überhaupt mit diesem Verfahren befasst war, ob der Betroffene zu Recht in den Kreis der Verdächtigen einbezogen werden durfte, so kann erst recht nicht der glaubhafte Schluss gezogen werden, es bestünde insofern eine Wiederholungsgefahr. Die Befugnis der Polizei eine Verdächtigendatei zu führen, ist nach § 30 Abs. 2 SPolG an Informationen geknüpft, „die sie im Rahmen von Strafermittlungsverfahren gewonnen hat". Inwieweit diese Voraussetzung erfüllt ist, lässt sich anhand eines staatsanwaltschaftlichen Aktenzeichens ersehen, denn die Polizei darf nicht eigenständig und dauerhaft die Tatsache eines Ermittlungsverfahrens dokumentieren, das möglicherweise nie stattgefunden hat.

Das Landeskriminalamt habe ich um Löschung von nicht verifizierbaren Daten aus den 80iger Jahren gebeten, da der Grundsatz der Unschuldsvermutung als Verfassungsgebot einzuhalten ist. Mir wurde versichert, dass bei anlassbezogenen Einzelfallprüfungen und Zweifeln an der Rechtmäßigkeit der Speicherungen diese Informationen unweigerlich gelöscht würden. Zweifel an der Rechtmäßigkeit der Speiche-

rung will das Landeskriminalamt aber nicht aus dem Fehlen eines Aktenzeichens oder einem völlig offenen Verfahrensausgang herleiten.

Aus datenschutzrechtlicher Sicht ergeben sich die Zweifel an der Rechtmäßigkeit der Speicherung jedoch bereits aus der gänzlich fehlenden Überprüfbarkeit der Speicherungen, die zur generellen Löschung von Straftaten Verdächtiger führen muss, die ohne staatsanwaltliches Aktenzeichen und ohne Vermerk über den Verfahrensausgang gespeichert sind.

Sollte die grundsätzliche Bereitschaft zur Löschung nicht verifizierbarer Daten auch weiterhin nicht bestehen, wird die Angelegenheit mit der Aufsichtsbehörde zu klären sein.

6 Verfassungsschutz

6.1 Änderungen im Verfassungsschutzgesetz

Das Terrorismusbekämpfungsgesetz des Bundes wurde wie in anderen Bundesländern so auch im Saarland in Landesrecht umgesetzt. Die im Terrorismusbekämpfungsgesetz vorgegebenen Bestimmungen sind dabei wortgleich übernommen worden.

Eine Regelung, die wenig Aufmerksamkeit bei der Änderung des Verfassungsschutzgesetzes im Jahre 2001 erregt hatte, fand aus Anlass der Terrorismusbekämpfung im Jahre 2003 ein nachhaltiges Medienecho.

Ich hatte – entgegen anders lautenden Pressedarstellungen – bereits 2001 den Wegfall einer Bestimmung gerügt, die eine umfassende Berücksichtigung von Zeugnisverweigerungsrechten bei der heimlichen Beobachtung durch den Verfassungsschutz vorsah. Diese lautete bis zum Jahre 2001 wie folgt:

> „Durch Maßnahmen des Landsamtes für Verfassungsschutz dürfen gesetzlich festgelegte Zeugnisverweigerungsrechte nicht beeinträchtigt werden."

Damit waren alle Zeugnisverweigerungsberechtigten, nicht nur Berufsgeheimnisträger (z.B. Ärzte, Journalisten) sondern u.a. auch Angehörige umfassend geschützt. Meine Bedenken gegen den Wegfall der Bestimmung fanden damals kein Gehör.

Im Zuge des Erlasses des Durchführungsgesetzes zum Terrorismusbekämpfungsgesetz und den damit verbundenen Diskussionen wurde publik, dass der Schutz der Zeugnisverweigerungsberechtigten im Verfassungsschutzgesetz nicht mehr verankert war. Neu aufgenommen wurde in das Gesetz sodann der auf die Berufsgeheimnisträger beschränkte Schutz von Zeugnisverweigerungsberechtigten, wenn diese nicht selbst als Verdächtige anzusehen sind.

Im Lichte der Entscheidungen des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung muss auch diese Begrenzung des Schutzes von Zeugnisverweigerungsberechtigten allein auf Berufsgeheimnisträger, unter Ausschluss der übrigen Zeugnisverweigerungsberechtigten, nicht zuletzt zur Wahrung des Kernbereichs privater Lebensgestaltung erneut im Sinne der alten Regelung aufgehoben werden.

7 Steuern

7.1 Durchbrechung des Steuergeheimnisses bei zwingendem öffentlichem Interesse

Die Zulässigkeit der Durchbrechung des Steuergeheimnisses ist nach § 30 Abgabenordnung an Hand keineswegs einfach formulierter Bestimmungen von den Finanzbehörden im Einzelfall zu prüfen. Ein Petent hat sich mit einem solchen Fall an mich gewandt. Der Betroffene sollte disziplinarrechtlich belangt werden. Im Rahmen dieses Verfahrens waren nach seiner Auffassung Steuerdaten von einer kommunalen Finanzkasse zu Unrecht an den Dienstherrn übermittelt worden. Er konnte um so eher von der Rechtswidrigkeit ausgehen, als zuvor das Finanzamt die Übermittlung seiner Daten unter Berufung auf das Steuergeheimnis abgelehnt hatte. Damit lagen zwei sich widersprechende Entscheidungen – wenn auch von unterschiedlichen Behörden – zu vergleichbaren Sachverhalten vor.

Bei beiden öffentlichen Stellen handelte es sich um Finanzbehörden, die an die Bestimmungen der Abgabenordnung gebunden sind. Dort sind die Voraussetzungen aufgelistet, nach denen ein Amtsträger Steuerdaten befugt offenbaren darf oder aber das Steuergeheimnis verletzt.

Ungeachtet der Befürchtung, dass der kommunalen Finanzbehörde der Stellenwert des Steuergeheimnisses als besonderes Amtsgeheimnis nicht ausreichend bewusst war, hätte an Hand der Tatbestände, die der Gesetzgeber für die zulässige Offenbarung normiert hat, eine sorgfältige Bewertung durch die Behörde vorgenommen werden müssen.

Zu prüfen war die Frage, ob hier ein „zwingendes öffentliches Interesse“ an der Offenbarung der Steuerdaten bestand. In welchen Fällen ein zwingendes öffentliches Interesse anzunehmen ist, hat der Gesetzgeber an Fällen dargestellt, die angesichts ihrer Schwere als Straftat oder ihrer Bedeutung für die Öffentlichkeit eine Durchbrechung des Steuergeheimnisses rechtfertigen können.

Die sorgfältige Prüfung der gesetzlichen Voraussetzungen konnte nur zu dem Ergebnis führen, dass die zur Rede stehenden etwaigen disziplinarrechtlichen Verfehlungen keine Vergleichbarkeit mit den im Gesetz aufgeführten Verbrechen, vorsätzlichen schweren Vergehen gegen Leib und Leben oder solche Straftaten gegen den Staat und seine Einrichtungen aufzeigten. Erhebliche Wirtschaftsstraftaten standen ebenfalls nicht zur Debatte.

Das Verfahren befand sich zudem im Stadium der disziplinarischen Vorermittlungen, in denen erst geprüft werden soll, ob ausreichend gesicherte Tatsachen den Verdacht eines Dienstvergehens zwecks Eröffnung eines Disziplinarverfahrens zu erhärten vermögen. Auch dieser Sachverhalt war für die Bewertung von Bedeutung, denn ein (Steuer-)Strafverfahren war gegen den Petenten nicht eingeleitet, aus dem sich die Vergleichbarkeit mit den im Raum stehenden Vorwürfen ohne Zweifel hätte ergeben können. Der Vorermittlungsführer versuchte in diesem Zusammenhang lediglich den Verdacht des leichtfertigen Schuldenmachens und den Vorwurf einer fehlenden Nebentätigkeitsgenehmigung zu klären.

Ich habe der Behörde dargestellt, welche Rechtsfragen vor einer Durchbrechung des Steuergeheimnisses auf der Grundlage eines zwingenden öffentlichen Interesses zu prüfen sind. Das Gefühl, jegliches Fehlverhalten eines Beamten bedürfe einer Sanktion, darf hier – jenseits der Festlegungen des Gesetzgebers – keinesfalls den Ausschlag geben.

7.2 Staatliche Kontenkontrolle

Bankkunden genießen nach § 30 a Abgabenordnung (AO) einen besonderen Schutz; deshalb gebietet die Regelung Rücksichtnahme auf das Vertrauensverhältnis zwischen den Kreditinstituten und deren Kunden bei der Ermittlung eines steuerrelevanten Sachverhalts durch Finanzbehörden.
In den heutigen Zeiten leerer Kassen der öffentlichen Hand werden an der Rücksichtnahme auf das privatrechtlich vereinbarte Bankgeheimnis deutliche Abstriche gemacht. Es kann aus der Sicht des Datenschutzes nicht darum gehen, Steuer- oder

Sozialleistungssünder vor Entdeckung zu bewahren. Aber ebenso wie der potentielle Straftäter aus dem Gesetz bei bestimmten Verhaltensweisen ablesen können muss, was der Staat erlaubt und kontrollieren kann, so sind auch Steuergesetze normenklar und so bestimmt zu fassen, dass jeder erkennen kann, wie ein staatliches Verwaltungsverfahren ablaufen wird. Dies kann zudem eine abschreckende Wirkung auf potentielle Steuersünder entfalten.

Den Voraussetzungen an ein normenklares, transparentes Gesetz wird das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.03 (BGBl. I 2003, S. 2928) in einigen Punkten nicht gerecht. Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung die Defizite aufgeführt und eine Überarbeitung dieser Regelungen gefordert (Anlage 15.24).

In allererster Linie wäre zu prüfen und darzustellen, wie die neuen Bestimmungen mit dem Gebot der Rücksichtnahme auf das Bankgeheimnis nach § 30 a AO in Einklang zu bringen sind.

Das Bundesverfassungsgericht hat zwar kürzlich im Verfahren einer einstweiligen Anordnung, das Beschwerdeführer einer noch anhängigen Verfassungsbeschwerde vorgeschaltet hatten, das Inkrafttreten des Gesetzes zum 1.4.2005 nicht ausgesetzt. Dazu beigetragen hat maßgeblich ein Erlass des Bundesfinanzministeriums, der sowohl das einheitliche Vorgehen der Finanzverwaltung als auch die zulässige Kontendatenabfrage durch andere Behörden regelt. Außerdem sieht der Erlass die Benachrichtigung Betroffener nach einem Kontendatenabruf vor.

Die jetzige Rechtslage bleibt dennoch mehr als unbefriedigend. Durch den Erlass der Finanzverwaltung werden andere Behörden außerhalb der Finanzverwaltung nicht gebunden. Im Gegensatz zu einer gesetzlichen Regelung vermag der Erlass auch nicht die in Rede stehende Verfassungswidrigkeit eines Gesetzes zu bereinigen. Hinzu kommt, dass die Verwaltung ihn jederzeit ohne parlamentarische Erörterungen abändern oder aufheben kann. Auf dem Erlasswege kann mithin die erforderliche Rechtssicherheit und auch die Normenklarheit nicht hergestellt werden. Der Gesetzgeber sollte sich mit der Materie nochmals befassen und insbesondere wesentliche Elemente des Datenschutzes, wie z.B. die Benachrichtigung über einen Kontenda-

tenabruf, in das Gesetz aufnehmen, sofern das Bundesverfassungsgericht im Hauptsacheverfahren die Vereinbarkeit mit der Verfassung bestätigt.

8 Soziales

8.1 Aufbewahrungsfristen für Akten des Jugendamtes

Ein Kreisjugendamt beabsichtigte, die Aufbewahrungsdauer der Akten des Bezirkssozialdienstes neu zu regeln und dabei die Fristen gegenüber der bisherigen Praxis – auch anderer Jugendämter – wesentlich zu verkürzen. Dabei orientierte das Jugendamt sich an den Verjährungsfristen für Sozialleistungen und dem Grundsatz, dass Sozialdaten zu löschen sind, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt werden (§ 84 Absatz 2 SGB X).

So wurde grundsätzlich die Frist auf 5 Jahre nach Abschluss der Beratung/Hilfe, bei Hilfen zur Erziehung in ambulanter oder stationärer Form auf 10 Jahre nach Abschluss der Hilfe festgelegt. Ich habe diese Neuregelung befürwortet. Bei Adoptionsakten, die ursprünglich auf Dauer aufbewahrt werden sollten, wurde nach meinem Hinweis auf die Bestimmung des § 9 b Adoptionsvermittlungsgesetz (Neufassung vom 22.12.2001) die Frist auf 60 Jahre festgesetzt.

8.2 Datenspeicherung beim Jugendamt in einer Sorgerechtsangelegenheit

Ein getrennt lebender Ehemann legte dem Jugendamt umfangreiche Unterlagen, unter anderem Kopien von Krankenhausentlassungsberichten, ärztlichen Attesten und Arzneimittelverordnungen, privaten Schreiben, vor. Diese sollten beweisen, dass die Ehefrau nicht fähig sei, das Sorgerecht für das gemeinsame Kind wahrzunehmen. Die Ehefrau und deren Familie – bei einem Hausbesuch des Bezirkssozialarbeiters mit diesem „Beweismaterial“ konfrontiert – wollten von mir geklärt wissen, wie der Ehemann, ein Polizeibeamter, in den Besitz dieser Papiere gelangt sei und ob das Jugendamt berechtigt sei, sie in seinen Akten aufzubewahren.

Für den Verdacht, dass sich der Polizeibeamte in Ausnutzung seiner dienstlichen Funktion Unterlagen rechtswidrig beschafft hat, ergaben sich keine konkreten Hinweise. Das Jugendamt hat sich bereit erklärt, die für seine Aufgabenerfüllung nicht verwertbaren Unterlagen zu vernichten oder an die Betroffene zurückzugeben. Erst wenn das Familiengericht das Jugendamt bei der Sorgerechtsentscheidung beteiligt, werde das Amt die erforderlichen Informationen mit rechtlich zulässigen Mitteln beiziehen.

8.3 Hartz IV

Mit dem 1.1.2005 wurden die Arbeitslosenhilfe und die Sozialhilfe für erwerbsfähige Hilfebedürftige zusammengeführt. Dieser Personenkreis erhält nunmehr Leistungen nach dem II. Buch des Sozialgesetzbuches.
Neben Leistungen zur Eingliederung in Arbeit werden Leistungen zur Sicherung des Lebensunterhalts in Form des Arbeitslosengeldes II sowie Leistungen für Unterkunft und Heizung erbracht. Das Gesetz regelt, wer hilfebedürftig ist und in diesem Zusammenhang welches Einkommen und Vermögen zu berücksichtigen sind.
Die Voraussetzungen für den Erhalt der Leistungen unterscheiden sich wesentlich von den bisherigen Leistungsvoraussetzungen für Sozialhilfe und Arbeitslosenhilfe. Es mussten deshalb neue Antragsformulare entwickelt werden, mit denen die für die Leistung erheblichen Daten erfragt werden.
Als die Fragebogen im Sommer 2004 bekannt wurden, wurde schnell deutlich, dass diese erhebliche datenschutzrechtliche Defizite aufwiesen. Folgende Beispiele für besonders gravierende Datenschutzverstöße möchte ich nennen:

- Die Verdienstbescheinigung des Arbeitgebers befand sich zunächst auf der Rückseite der Einkommenserklärung des Antragstellers, womit der Arbeitgeber unnötigerweise von der sonstigen Einkommenssituation des Antragstellers Kenntnis nehmen konnte.
- In den Antragsformularen wird nicht klar zwischen Mitgliedern der Bedarfs- und der Haushaltsgemeinschaft unterschieden. Da über Mitglieder der Bedarfsgemeinschaft erheblich detailliertere Angaben erforderlich sind als bei sonstigen Mitbewohnern, kam es hier zu überflüssigen und damit unzulässigen Datenerhebungen.

- Erfragt werden Name, Anschrift und Bankverbindung des Vermieters, obwohl diese Angaben nur dann erforderlich sind, wenn die Miete ausnahmsweise direkt an den Vermieter überwiesen wird.

In Gesprächen der Datenschutzbeauftragten mit der Bundesagentur für Arbeit musste diese eingestehen, dass die Kritik weitgehend berechtigt war und hat zugesagt, künftig datenschutzgerechte Antragsbögen zu verwenden. Damit war aber den Arbeitslosen, die zum 1. Januar 2005 ihr Arbeitslosengeld II erhalten wollten, nicht gedient, denn sie waren gezwungen, die alten datenschutzwidrigen Formulare zu verwenden. Zur Schadensbegrenzung hat die Bundesagentur für Arbeit „Ausfüllhinweise“ herausgegeben, in denen erläutert wird, wie die Formulare datenschutzgerecht ausgefüllt werden können. Diese Ausfüllhinweise wurden an die Regionaldirektionen verschickt und im Internet veröffentlicht. Ich habe allerdings aufgrund verschiedener Eingaben bei meiner Dienststelle Zweifel, ob der Inhalt dieser Ausfüllhinweise bei jedem Sachbearbeiter tatsächlich angekommen ist.

Schon bald trat ein weiteres gravierendes datenschutzrechtliches Problem zutage: Der Einsatz des Datenbanksystems A2LL. Dieses System verfügt über keine Zugriffsberechtigungsverwaltung, was bedeutet, dass sämtliche Nutzer des Verfahrens auf alle erfassten Daten der Antragsteller auf Arbeitslosengeld II und weiterer in den Anträgen genannter Personen (z.B. Familienangehörige) zugreifen können, und das bundesweit. Die Zugriffsmöglichkeiten beschränken sich dabei nicht nur auf die Stammdaten dieser Personen, sondern auf sämtliche zur Bearbeitung automatisiert erfassten personenbezogenen Informationen. Eine Protokollierung der lesenden bundesweiten Suchanfragen, um Missbräuche auszuschließen bzw. nachträglich festzustellen, ist ebenso wenig möglich.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit in einer Entschließung vom 28./29. Oktober 2004 aufgefordert, die notwendigen Schritte zur Beseitigung der datenschutzrechtlichen Mängel unverzüglich einzuleiten (siehe Anlage 15.23). Der Bundesbeauftragte für den Datenschutz hat den Einsatz des Datenerhebungs- und Leistungsberechnungsprogrammes A2LL wegen Verstoßes gegen das Sozialgeheimnis beanstandet.

8.4 JobCard

Das Bundesministerium für Wirtschaft und Arbeit hat ein ehrgeiziges Projekt in Angriff genommen: Die Einführung einer so genannten JobCard.
Beantragt heute jemand die Gewährung von Leistungen bei öffentlichen Stellen (z.B. bei der Bundesagentur für Arbeit, Sozialamt usw.) müssen in vielen Fällen Arbeits- oder Verdienstbescheinigungen vorgelegt werden. Künftig sollen diese Daten zentral gespeichert und bei Bedarf mit der JobCard des Antragstellers abgerufen werden. Zusätzlich muss sich der Behördenmitarbeiter durch Einsatz seiner Signaturkarte legitimieren.
Dadurch soll ein Beitrag zur Entbürokratisierung der Verwaltung geleistet und der Einsatz der Signaturkarte gefördert werden. Insbesondere die Arbeitgeber und ihre Organisationen wollen sich von der Verpflichtung der Archivierung und dem Versand von Daten an eine Vielzahl verschiedener Stellen entledigen.
Durch das JobCard-Verfahren werden Millionen von Arbeitnehmerdaten bei einer zentralen Stelle gespeichert. Solche Zentraldateien mit umfangreichen Datensammlungen begründen erhebliche Gefahren. Nicht absehbare Zweckänderungen sowie andere Missbrauchsrisiken sind nie völlig auszuschließen. Es ist eine sorgfältige Risiko/Nutzen-Abwägung vorzunehmen, wobei auch zu berücksichtigen ist, dass hier Daten an die zentrale Speicherstelle übermittelt werden, die im Einzelfall nie benötigt werden, weil nicht jeder Bürger staatliche Leistungen in Anspruch nimmt.

Jedenfalls muss das Verfahren organisatorisch und technisch so ausgestaltet sein, dass unbefugte Zugriffe ausgeschlossen sind. Eine zentrale Frage ist in diesem Zusammenhang, ob die zentrale Speicherstelle die Möglichkeit haben darf, die Daten zu entschlüsseln oder ob nicht ein Verschlüsselungsmodell gewählt werden muss, das die Daten der Betroffenen mit seiner Signaturkarte bereits auf Arbeitgeberseite verschlüsselt, so dass die Daten auch nur mit seiner Mithilfe wieder entschlüsselt werden können (so genanntes Ende-zu-Ende-Verschlüsselungs-Modell). Auf ihrer Konferenz am 28./29. Oktober 2004 haben deshalb die Datenschutzbeauftragten des Bundes und der Länder beschlossen, das Bundesministerium für Wirtschaft und Arbeit zu bitten, einen neutralen Gutachter mit der Erstellung eines Gutachtens zur Realisierbarkeit des Ende-zu-Ende-Verschlüsselungs-Modells zu beauftragen.

8.5 Mitteilung des Sozialhilfebezugs an Vermieter

Ein Petent beschwerte sich bei meiner Dienststelle über ein Sozialamt wegen dessen Vorgehen in seiner Sozialhilfeangelegenheit. Der Petent hatte bei dem Sozialamt die Übernahme von zusätzlichen Heizkosten zu Lasten der Sozialhilfe beantragt. Die Höhe der Verbrauchskosten erschien dem zuständigen Sachbearbeiter sehr hoch. Zur Klärung der Ursache für die hohe Heizkostenrechnung setzte sich der Sachbearbeiter mit dem Vermieter des Petenten in Verbindung. Dieser bestätigte, dass der Verbrauch des Petenten fast doppelt so hoch sei wie bei dessen Vormieter; er könne sich dies nur damit erklären, dass es in der Wohnung des Petenten immer sehr warm sei.
Der Petent sieht in diesem Vorgehen eine Verletzung des Sozialgeheimnisses, da sein Vermieter durch den fraglichen Anruf zum ersten Mal davon Kenntnis erlangt habe, dass er Sozialhilfebezieher sei. Das Sozialamt rechtfertigt seine Vorgehensweise damit, dass aus den von dem Petenten zugesandten Unterlagen ein Grund für einen derart hohen Energieverbrauch nicht erkennbar gewesen sei.

Nach Prüfung der Rechtslage bin ich zu dem Ergebnis gekommen, dass eine unzulässige Datenübermittlung nicht vorgelegen hat. Das Verfahren bei der Ermittlung des Sachverhaltes durch Sozialleistungsträger ist im Sozialgesetzbuch X geregelt. Nach § 67 a Abs. 2 Satz 1 dieses Gesetzes sind Sozialdaten grundsätzlich beim Betroffenen zu erheben. Ausnahmsweise dürfen Sozialdaten aber auch bei anderen Personen erhoben werden, wenn unter anderem die Aufgaben nach diesem Gesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 67 a Abs. 2 Nr. 2 b) aa)). Aus den vorgelegten Verbrauchsabrechnungen konnte der Sachbearbeiter ersehen, dass die Energiekosten außergewöhnlich hoch waren. Eine Übernahme dieser hohen Kosten wäre möglicherweise in Betracht gekommen, wenn die Ursache bei der Heizungsanlage (defekt, veraltet) gelegen hätte. Insofern war der Hinweis des Vermieters – den nur dieser geben konnte – über die Heizkosten des Vormieters erheblich für die Entscheidung über die Übernahme der Heizkosten durch das Sozialamt.

8.6 Unnötige Versendung von Sozialakten zur Gewährung von Akteneinsicht

Die Akteneinsicht ist grundsätzlich bei der Behörde wahrzunehmen, die die Akten führt. In besonderen Fällen kann die Sozialbehörde die Akteneinsicht auch bei einer anderen Stelle gestatten (§ 25 Abs. 4 SGB X). Um einen solchen Ausnahmefall handelte es sich bei dem Empfänger von Sozialleistungen, der sich mit einer Beschwerde an mich wandte.

Das Landesamt für Jugend, Soziales und Versorgung hatte seinen Antrag auf Akteneinsicht bewilligt und – ohne mit dem Antragsteller zuvor Kontakt aufzunehmen – die Versorgungsakten an die Wohnsitzgemeinde übersandt. Das Amt handelte wohl in guter Absicht, um dem in einem anderen Bundesland wohnenden Leistungsempfänger die Akteneinsicht in seiner Nähe zu ermöglichen. Der Antragsteller wunderte sich, dass die Akten „ohne Ankündigung plötzlich“ versandt wurden. Er teilte mit, dass er die Akteneinsicht aus gesundheitlichen Gründen bei der Gemeindeverwaltung nicht wahrnehmen könne. Ich sehe in der Versendung von Sozialakten mit sehr sensiblen Angaben über die gesundheitlichen und finanziellen Verhältnisse ohne vorherige Beteiligung des Antragstellers eine nicht erforderliche und deshalb unzulässige Datenübermittlung.

Das Landesamt hält seine Verfahrensweise für rechtmäßig. Es betont, dass die Entscheidung über die Gewährung von Akteneinsicht bei einer anderen Stelle im Ermessen der Sozialbehörde liege. Vorab habe die betreffende Gemeindeverwaltung auf telefonische Anfrage versichert, dass der Antragsteller bei seiner Akteneinsicht genügend Pausen einlegen könne und die Zugänge zu den Diensträumen ohne Probleme zu erreichen seien. Warum die Sozialbehörde den Antragsteller nicht selbst befragt hat, wird nicht dargelegt. Sie verweist darauf, dass auch die Bediensteten der Gemeindeverwaltung zur Verschwiegenheit verpflichtet seien und eine Verarbeitung der Daten bei dieser Stelle nicht erfolge. Insoweit würden die §§ 67 b ff SGB X hier nicht greifen.

Dieser Auffassung muss ich widersprechen. Die Behörde hat das Ermessen, ob sie Akteneinsicht bei einer anderen Stelle gewährt, in pflichtgemäßer Weise auszuüben. Insbesondere ist von dem Ermessen in einer dem Zweck der Ermächtigung entsprechenden Weise Gebrauch zu machen. Zweck der Regelung des § 25 Abs. 4 Satz 2

SGB X ist, dem Antragsteller, der aus besonderen Gründen an der Akteneinsicht beim Leistungsträger verhindert ist, dennoch die Einsichtnahme zu ermöglichen. Das Recht auf Akteneinsicht kann nur dann erfolgreich wahrgenommen werden, wenn diese zu Bedingungen angeboten wird, die der Antragsteller erfüllen kann. Wünschen des Berechtigten soll entsprochen werden, soweit sie angemessen sind (vgl. § 33 SGB I). Daraus folgt, dass – um eine unnötige Aktenübersendung zu vermeiden – die Einschaltung einer anderen Behörde nur nach Anhörung des Betroffenen erfolgen darf. Im Übrigen ist eine ohne Rechtsgrundlage erfolgte Datenübermittlung auch dann rechtswidrig, wenn der Datenempfänger zur Verschwiegenheit verpflichtet ist.

Ich habe die Aufsichtsbehörde, das Ministerium für Justiz, Gesundheit und Soziales gebeten, das Landesamt anzuweisen, in solchen Fällen künftig stets den Antragsteller zu der beabsichtigten Aktenübersendung zu hören.

8.7 Vorlage von Kontoauszügen beim Sozialamt

Ein Petent hatte einen Antrag auf Sozialhilfe gestellt. Das Sozialamt machte die Bearbeitung des Antrages von der Vorlage der Kontoauszüge der letzten 2 Monate abhängig.
Der Petent sieht in diesem Verlangen einen unverhältnismäßigen Eingriff in seine Persönlichkeitsrechte, weil bei Abbuchungen meist der Verwendungszweck angegeben ist und das Sozialamt so einen recht tief gehenden Einblick in die Lebensweise eines Antragstellers erhält. Man denke nur beispielsweise an Mitgliedsbeiträge an Parteien oder Spenden für bestimmte Organisationen. Ein solcher Eingriff in seine Privatsphäre könne nur bei Vorliegen eines konkreten Anfangsverdachtes eines Sozialhilfemissbrauchs gerechtfertigt sein.
Im Grundsatz hat der Petent damit die Problematik der Vorlage von Kontoauszügen bei Beantragung staatlicher Leistungen zutreffend beschrieben. In seinem konkreten Fall hatte ich allerdings gegen die Verfahrensweise des Sozialamtes keine datenschutzrechtlichen Bedenken. Das Sozialamt hat in seiner Stellungnahme das Verlangen nach Vorlage der Kontoauszüge damit gerechtfertigt, dass der Petent in seinem Sozialhilfeantrag angegeben hatte, Eigentümer eines PKW zu sein. Somit habe der Verdacht bestanden, er könnte über zusätzliches Einkommen verfügen. Darüber

hinaus hat das Sozialamt mitgeteilt, dass gegen eine Schwärzung der Soll-Buchungen keine Bedenken bestünden; im Übrigen sei es Praxis, die Kontoauszüge nicht zu den Akten zu nehmen, sondern den Antragstellern wieder zurückzugeben.

Es bestand somit im konkreten Fall keine Veranlassung für ein weiteres Tätigwerden meiner Dienststelle.

9 Gesundheit

9.1 Änderung des Saarländisches Rettungsdienstgesetzes

Zu dem Entwurf wurde mir Gelegenheit zur Stellungnahme gegeben. In dem inzwischen verabschiedeten Gesetz wird klargestellt, dass bei der Rettungsleitstelle eingehende Anrufe vorübergehend auf Datenträger aufgezeichnet werden dürfen. Die Aufzeichnungen sind spätestens nach 6 Monaten zu löschen, sofern sie nicht als Beweismittel benötigt werden. Positiv gewertet habe ich auch die Regelung, bei der Dokumentation anfallende Daten für Zwecke der Qualitätssicherung und Effizienzkontrolle lediglich in nichtpatientenbezogener Form auszuwerten.

9.2 Angabe der Diagnose für den Krankentransport

Ein Krankenhausarzt hat bei mir angefragt, ob es richtig sei, beim Transport von Patienten in eine andere Klinik oder nach Hause dem Rettungssanitäter die genauen Diagnosen der zu transportierenden Person mitzuteilen. Dies sei allgemeine Praxis in den Krankenhäusern. Nach Auffassung des Klinikarztes reicht es aus, dem Krankentransportpersonal mitzuteilen, ob durch den Transport für sie selbst oder den Patienten eine Gefährdung besteht (z.B. die Möglichkeit einer Infektion) und auf welche besonderen Umstände zu achten ist.
Ich habe den Arzt in seiner kritischen Einstellung zur Wahrung der ärztlichen Schweigepflicht bestärkt. Eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses ist nach § 29 Abs. 4 Satz 1 Saarländisches Krankenhausgesetz unter anderem nur dann zulässig, soweit dies für die Durchführung der Behandlung des Patienten erforderlich ist. Das Krankentransportpersonal benötigt sicherlich nicht die exakten Diagnosen. Die vom Klinikarzt genannten Informationen reichen auch aus meiner Sicht aus, den Krankentransport ordnungsgemäß durchzuführen.

Neue Formulare für Krankenfahrten mit dem Taxi haben im Berichtszeitraum für Aufregung und zahlreiche Presseartikel gesorgt. Die Kosten für solche Fahrten werden nach der Gesundheitsreform nur noch in bestimmten Fällen und nach Genehmigung durch die Krankenkasse übernommen. In der dem Taxifahrer auszuhändigenden „Verordnung über Krankenbeförderung“ hatte der behandelnde Arzt auch die Diagnose einzutragen.
Inzwischen wurde ein datenschutzgerechtes Verfahren gefunden, das ausschließt, dass dem Taxifahrer medizinische Details zur Kenntnis gelangen.

9.3 Datenübermittlung vom Gesundheitsamt an das Krebsregister

Für das beim Ministerium für Justiz, Gesundheit und Soziales geführte Epidemiologische Krebsregister ist die Kenntnis des Sterbedatums und der Todesursache zur Bewertung der Effektivität des Gesundheitswesens unabdingbar.

Damit dieser Datenbedarf befriedigt werden kann, regelt das Saarländische Krebsregistergesetz im Einzelnen, welche Daten verschiedene Behörden, wie die Gesundheitsämter, das Statistische Landesamt oder die Meldebehörden an das Krebsregister zu übermitteln haben.
Im Berichtszeitraum habe ich von einer „Kooperationsvereinbarung zwischen dem Epidemiologischen Krebsregister Saarland und den saarländischen Gesundheitsämtern“ Kenntnis erlangt, in dem sich die Gesundheitsämter verpflichten, dem Krebsregister monatlich alle Leichenschauscheine zur Erfassung der relevanten Daten zu überlassen. Die Problematik dieser Verfahrensweise besteht darin, dass die Leichenschauscheine mehr Daten enthalten, als die Gesundheitsämter nach den Vorschriften des Krebsregistergesetzes übermitteln müssen, dass also dem Krebsregister zu seiner Aufgabenerfüllung nicht erforderliche Daten zur Kenntnis gelangen. Als Begründung für die von dem Gesetz abweichende Verfahrensweise hat das Krebsregister die Arbeitsersparnis für die Gesundheitsämter angeführt, die ansonsten mangels Personals nicht in der Lage wären, die im Krebsregistergesetz aufgeführten Daten zu liefern.

Eine Beanstandung habe ich unter dem Vorbehalt zurückgestellt, dass das Krebsregistergesetz in absehbarer Zeit so geändert wird, dass die geübte Praxis im Gesetz ihren Niederschlag findet.

Ich erwarte, dass von Seiten des zuständigen Ministeriums eine entsprechende Gesetzesnovellierung in die Wege geleitet wird.

9.4 Elektronische Gesundheitskarte

Mit dem am 1. Januar 2004 in Kraft getretenen Gesundheitsmodernisierungsgesetz wurde auch ein neuer § 291 a in das SGB V aufgenommen, wonach die bisherige zu administrativen Zwecken (Berechtigungsnachweis, Abrechnung mit den Leistungserbringern) verwandte Krankenversichertenkarte bis zum 1. Januar 2006 zu einer elektronischen Gesundheitskarte erweitert werden soll.

Die Karte wird einen Pflichtteil mit den administrativen Daten der bisherigen Krankenversichertenkarte (Name, Anschrift, Geburtsdatum, Krankenkasse, Versichertenstatus, Versichertennummer) sowie die Möglichkeit zur papierlosen Übertragung von Rezepten beinhalten. In einem freiwilligen medizinischen Teil der Karte können Notfalldaten, wie z.B. Blutgruppe, chronische Erkrankungen oder Allergien gespeichert werden; darüber hinaus Befunde, Diagnosen, Therapieempfehlungen und -maßnahmen, Behandlungsberichte, Impfungen, Röntgenuntersuchungen usw. Gespeichert werden können auch von den Versicherten selbst zur Verfügung gestellte Daten, wie z.B. Hinweise auf Patientenverfügungen sowie Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten.

Es wird nun darauf ankommen, die Vorgaben des Gesetzgebers, die in hohem Maße datenschutzfreundlich sind, in die Praxis umzusetzen. Zu nennen sind hier insbesondere folgende Gesichtspunkte, die die Datenhoheit der Versicherten gewährleisten sollen:

- Verarbeitung von Patientendaten im medizinischen Teil der Karte nur mit ausdrücklicher Einwilligung der Versicherten, wobei die Einwilligung jederzeit widerruflich ist.

- Möglichkeit, die Einwilligung auf einzelne Anwendungen zu beschränken sowie Entscheidungsmöglichkeit, welche Daten konkret erfasst werden sollen.
- Wahlmöglichkeit, wer Zugriff auf welche Informationen haben soll.
- Zugriffsrecht auf die medizinischen Daten nur für Ärzte, Apotheker und Angehörige anderer Heilberufe und dies auch nur in Verbindung mit einem elektronischen Heilberufeausweis oder entsprechenden Berufsausweis, die über eine qualifizierte elektronische Signatur verfügen.
- Löschung der Daten auf Verlangen der Versicherten.
- Protokollierung für Zwecke der Datenschutzkontrolle.
- Keine Verpflichtung, die Karte Arbeitgebern oder Versicherungen vorzulegen.

Die Arbeiten zur Umsetzung der elektronischen Gesundheitskarte sind in vollem Gange. In Modellprojekten in einzelnen Bundesländern sollen demnächst erste Erfahrungen beim Umgang mit der Gesundheitskarte gesammelt werden. Die Datenschutzbeauftragten des Bundes und der Länder haben eine Arbeitsgruppe eingesetzt, die die einzelnen Verfahrensschritte kritisch begleitet.

9.5 Gesundheitsmodernisierungsgesetz

Am 1. Januar 2004 ist das in der Öffentlichkeit viel diskutierte Gesundheitsmodernisierungsgesetz in Kraft getreten.
Einen Punkt, der zu einer Verschlechterung im Hinblick auf die Daten der gesetzlich Krankenversicherten geführt hat, möchte ich herausgreifen: Bisher war es so, dass die Kassenärztlichen Vereinigungen, die für die Abrechnung der ambulanten Behandlungen mit den Ärzten zuständig sind, den Krankenkassen nur nichtversichertenbezogene Angaben über ihre Abrechnungen mitteilen mussten. Dies hatte der Gesetzgeber in der alten Fassung des § 295 SGB V wie folgt zum Ausdruck gebracht: „Für die Abrechnung der Vergütung übermitteln die Kassenärztlichen Vereinigungen den Krankenkassen, auf Verlangen auf Datenbändern oder anderen maschinell verwertbaren Datenträgern, für jedes Quartal die für die vertragsärztliche Versorgung erforderlichen Angaben über die abgerechneten Leistungen fallbezogen, nicht versichertenbezogen."

Mit der ab 1. Januar 2004 geltenden Neuregelung ist die Einschränkung, dass die Angaben nur fallbezogen an die Krankenkassen mitgeteilt werden dürfen, entfallen. Damit ist die Situation entstanden, dass die Krankenkassen umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten, die ihnen bisher nicht zugänglich waren. Auch wenn diese Neuregelung ihren Grund in der grundsätzlichen Änderung des bisherigen Vergütungssystems (Ablösung der Gesamtvergütung durch Regelleistungsvolumina) hat, bleibt als Ergebnis festzuhalten, dass die Gefahr gläserner Patientinnen und Patienten näher rückt.

Glücklicherweise ist es wenigstens noch gelungen, den Ausschuss für Gesundheit und Soziale Sicherheit des Bundestages zu einer Klarstellung zu bewegen, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist und dass die Krankenkassen die Daten nur für Abrechnungs- und Prüfungszwecke nutzen dürfen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich auf ihrer Tagung am 25./26. September 2003 in einer Entschließung (siehe Anlage 15.12) u.a. mit dieser Thematik befasst.

9.6 Herausgabe von Patientenunterlagen

Datenschutzbeauftragte von Krankenhäusern tragen dem Landesbeauftragten häufig Probleme vor, die sich im Klinikalltag stellen. Dazu folgende Auswahl:

- Verwandte von Patienten sprechen vor und verlangen die Herausgabe von Arztbriefen oder Röntgenbildern zur Vorlage beim nachbehandelnden Arzt. Sie behaupten, im Auftrag der Patienten, die meist bereits entlassen sind, zu handeln.
  Ich halte eine Herausgabe von Patientenunterlagen an Angehörige oder sonstige Dritte nur dann für zulässig, wenn die betreffende Person eine Vollmacht des ehemaligen Patienten vorlegt und sich durch ein Ausweispapier legitimiert. Nur so kann weitgehend sichergestellt werden, dass sensible Patientenunterlagen nicht in unbefugte Hände gelangen. Ich verkenne nicht, dass diese Verfahrensweise im Einzelfall auf Unverständnis stößt. Andererseits ist es keinem Krankenhausmitarbeiter zuzumuten, sich dem Vorwurf einer Verletzung der ärztlichen Schweige-

pflicht mit entsprechenden strafrechtlichen Konsequenzen auszusetzen. Im Einzelfall ist es eventuell auch möglich, bei dem betreffenden Patienten fernmündlich nachzufragen, ob er mit der Herausgabe seiner Unterlagen an die vorsprechende Person einverstanden ist.

- Im Krankenhaus wird der Patient befragt, an welchen Arzt (Hausarzt, weiterbehandelnder Arzt) Patientenunterlagen übermittelt werden sollen. Oft geht der Patient jedoch nach der Entlassung tatsächlich zu einem anderen Arzt zur Weiterbehandlung. Wie hat sich das Krankenhaus zu verhalten, wenn nunmehr ein solcher, ursprünglich nicht benannter Arzt fernmündlich Patientenunterlagen anfordert? Muss eine schriftliche Einwilligung des Patienten vorgelegt werden?
  Ich habe die Auffassung vertreten, dass auch dann, wenn der Patient im Krankenhaus bestimmte Ärzte benannt hat, weiteren Ärzten für die Weiterbehandlung erforderliche Berichte zur Verfügung gestellt werden dürfen. Die Voraussetzungen für eine solche Weitergabe richten sich nach den Bestimmungen der Berufsordnung für die Ärztinnen und Ärzte des Saarlandes. § 9 Abs. 4 der Berufsordnung bestimmt, dass für den Fall, dass mehrere Ärzte nacheinander denselben Patienten behandeln, sie untereinander insoweit von der Schweigepflicht befreit sind, als das Einverständnis des Patienten vorliegt oder anzunehmen ist. Die Vorlage eines schriftlichen Einverständnisses sieht die Berufsordnung nicht vor. Dies ist im Regelfall wohl akzeptabel. Allerdings sollte das Krankenhauspersonal auf der Vorlage einer schriftlichen Einverständniserklärung bestehen, wenn aufgrund irgendwelcher Umstände zu bezweifeln ist, dass der anfordernde Arzt in die Behandlung des Patienten eingebunden ist oder Anhaltspunkte dafür vorliegen, dass der Patient eine Information dieses Arztes nicht wünscht.

9.7 Novellierung des Saarländischen Krankenhausgesetzes

Im Berichtszeitraum hatte ich Gelegenheit, zu dem Referentenentwurf eines Gesetzes zur Neufassung des Saarländischen Krankenhausgesetzes aus datenschutzrechtlicher Sicht Stellung zu nehmen. Ein Novellierungsbedarf ist entstanden durch die Einführung eines neuen Vergütungssystems durch das Fallpauschalengesetz aus dem Jahre 2002, wonach nicht mehr der von der Patientin oder dem Patienten im

Krankenhaus verbrachte Tag, sondern die konkrete Leistung unabhängig von der Verweildauer bezahlt wird.

Bei Durchsicht des Gesetzentwurfs habe ich positiv registriert, dass die bisherigen detaillierten Regelungen zur Verarbeitung von Patientendaten im Krankenhaus praktisch unverändert beibehalten werden sollen. Die Vorschriften waren das Ergebnis intensiver Diskussionen mit dem damaligen Gesundheitsministerium und haben sich in der Praxis seit nunmehr fast 20 Jahren bewährt. Ich begrüße deshalb, dass Sie nicht den heute – vielfach festzustellenden – Bestrebungen nach Deregulierung zum Opfer gefallen sind.

In der Praxis hat sich allerdings auch gezeigt, dass es Notwendigkeiten zur Nutzung von Patientendaten gibt, die von den Datenschutzbestimmungen nicht gedeckt waren. So werden beispielsweise qualitätssichernde Maßnahmen häufig von Stellen außerhalb des Krankenhauses durchgeführt. Eine entsprechende Übermittlungsbefugnis ist im bisherigen Krankenhausgesetz nicht enthalten. Ich habe deshalb im Rahmen meiner Anhörung vorgeschlagen, eine Befugnisnorm aufzunehmen, die es dem Krankenhaus erlaubt, zu Zwecken der Qualitätssicherung Patientendaten nach außen zu geben. Ich habe dies allerdings von den Voraussetzungen abhängig gemacht, dass der Empfänger eine Ärztin oder ein Arzt oder zumindest eine ärztlich geleitete Stelle ist, dass der genannte Zweck nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden kann und nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

Auch die Technik hat sich seit Erlass des Krankenhausgesetzes im Jahre 1987 weiter entwickelt. So erscheint mir die Regelung, dass Patientendaten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufs gespeichert sind, unmittelbar nach Abschluss der Behandlung zu löschen sind, heute nicht mehr zeitgemäß. Andererseits ist es ein berechtigtes Anliegen des Datenschutzes, dass nach Abschluss der Behandlung der Kreis der Personen im Krankenhaus, die Zugriff auf Behandlungsdaten haben, eingeschränkt ist. Ich habe deshalb eine Regelung vorgeschlagen, wonach personenbezogene Daten, die in automatisierten Verfahren gespeichert und direkt abrufbar sind, nach Abschluss der Behandlung dem alleinigen Zugriff der jeweiligen Fachabteilung unterliegen. Nur mit Zustimmung der Fachabteilung und bei

Erforderlichkeit zur Durchführung der (erneuten) Behandlung darf der Direktzugriff auch für andere Stellen im Krankenhaus eröffnet werden.

Das zuständige Ministerium für Justiz, Gesundheit und Soziales hat mir signalisiert, dass es meine Regelungsvorschläge aufgreifen will.

9.8 Psychotherapeutenkammer des Saarlandes

Durch eine Änderung des Heilberufekammergesetzes wurde die Psychotherapeutenkammer des Saarlandes errichtet. Zu den Entwürfen für die Wahlordnung zur Vertreterversammlung, zur Meldeordnung und zum Meldebogen habe ich aus datenschutzrechtlicher Sicht Stellung genommen. Meine Vorschläge hat das Ministerium weitgehend aufgegriffen.

9.9 Schülerbefragung durch den Jugendärztlichen Dienst

Die saarländischen Gesundheitsämter führen im Rahmen der Schulgesundheitspflege in den 4. und 8. Klassen Untersuchungen der Schülerinnen und Schüler durch. Neuerdings werden an die Jugendlichen der 8. Klasse im Zusammenhang mit diesen Untersuchungen Fragebogen ausgeteilt, in denen nach Frühstücksgewohnheiten, gesundheitlichen Beschwerden, der sexuellen Aufklärung, dem Alkohol-, Zigaretten- oder Drogenkonsum, sportlichen Aktivitäten, dem Freizeitverhalten wie Computernutzung und Musikhören, Stimmungen, Problemen mit anderen Menschen usw., gefragt wird. Die Teilnahme an der Befragung ist freiwillig. Es wird in dem Fragebogen auch darauf hingewiesen, dass die Antworten nur anonymisiert, nämlich ohne Namen und Adresse, gespeichert werden.
Allerdings musste ich die Fachaufsichtsbehörde für die Gesundheitsämter, das Ministerium für Justiz, Gesundheit und Soziales, darauf aufmerksam machen, dass die Befragung nicht als anonym, sondern als personenbezogen anzusehen ist. Den Schulärzten, die den ausgefüllten Fragebogen entgegennehmen, ist die Identität des betreffenden Schülers bekannt. Außerdem werden die Bogen zusammen mit den Ergebnisblättern der schulärztlichen Untersuchung aufbewahrt, bis die Daten in ei-

nem Statistikprogramm in anonymisierter Form erfasst werden. Erst dann werden die Fragebogen vernichtet.
Auf diese Verfahrensweise ist in dem Erläuterungsteil des Fragebogens hinzuweisen. Daneben sind die Erziehungsberechtigten im Elternbrief über die Befragung zu informieren. Schließlich werden nicht nur äußerst sensible Daten ihrer minderjährigen Kinder erfragt, sondern auch Angaben, die über Erziehung und Verhältnisse im Elternhaus Aufschluss geben (z.B. sexuelle Aufklärung durch Eltern, Mitnahme des Schulfrühstücks von zuhause, Zeit für Fernsehkonsum und Computernutzung). Die Schülerinnen und Schüler dürfen daher nur dann an der Befragung teilnehmen, wenn die Erziehungsberechtigten ihre Einwilligung erteilt haben.
Das Ministerium hat zugesichert, die datenschutzrechtlichen Anforderungen einzuhalten.

9.10 Sozialdatenschutz bei stationärer Behandlung von Mitarbeitern der Krankenkasse

Beschäftigte gesetzlicher Krankenkassen sind regelmäßig auch bei ihrem Arbeitgeber krankenversichert. Um zu verhindern, dass die Personalstellen oder die unmittelbaren Kollegen Kenntnis von Krankheitsdaten erhalten, werden organisatorische Maßnahmen zur Abschottung der Sozialdaten der Mitarbeiter getroffen (vgl. § 35 Abs. 1 Satz 3 SGB I). So hat eine große Ersatzkasse eine zentrale Mitarbeiter-Geschäftsstelle gebildet, an die z.B. bei Krankenhausbehandlungen von Beschäftigten Kostenübernahmeanträge, Verlängerungsanträge oder Entlassungsanzeigen zu senden sind. Der Krankenhauseinweisung wird ein spezielles Merkblatt beigeheftet, das auf das Verfahren mit Angabe der zentralen Postadresse hinweist.
Ein saarländisches Krankenhaus ignorierte nach Mitteilung eines Betroffenen grundsätzlich diese Regelung und sandte in seinem Falle die Krankenhauseinweisung mit der Diagnose an die Beschäftigungsstelle. Das Krankenhaus hat auf meine Nachfrage diese Verletzung des Sozialdatenschutzes als Einzelfall dargestellt. Die Beschwerde wurde jedoch zum Anlass genommen, alle in Frage kommenden Stellen der Klinik zu verpflichten, die datenschutzrechtlichen Vorgaben einzuhalten.

9.11 Weitergabe von Patientendaten an die Kassenärztliche Vereinigung; Plausibilitätsprüfung der Honorarabrechnung

Mehrere Ärzte haben im Berichtszeitraum bei mir angefragt, ob sie sich möglichweise wegen Verletzung der ärztlichen Schweigepflicht strafbar machen, wenn sie der Kassenärztlichen Vereinigung, wie von dieser gefordert, personenbezogene Patientenunterlagen vorlegen.
Die Kassenärztliche Vereinigung hatte eine Stichprobe von Ärzten gezogen und diese aufgefordert, sämtliche in ihrer Praxis befindlichen Karteikarten einschließlich aller dazugehörigen Unterlagen, wie Anästhesieprotokolle, Krankenblätter, fachspezifische Dokumentationen sowie Befundberichte von in einer Liste aufgeführten Patienten zur Durchführung einer Plausibilitätsprüfung vorzulegen.

Strafbar nach § 203 Abs. 1 Nr. 1 StGB macht sich ein Arzt, der „unbefugt“ ein ihm anvertrautes Geheimnis offenbart. Wenn eine Befugnis zur Datenoffenbarung besteht, liegt keine Verletzung der ärztlichen Schweigepflicht vor. Eine solche Befugnis ergibt sich insbesondere aus gesetzlichen Vorschriften.
Der Gesetzgeber hat im Sozialgesetzbuch 5. Buch – Gesetzliche Krankenversicherung – (SGB V) den Krankenkassen und Kassenärztlichen Vereinigungen die Berechtigung eingeräumt, die sachliche und rechnerische Richtigkeit der Abrechnungen sowie die Wirtschaftlichkeit der ärztlichen Tätigkeit zu überprüfen.
Im konkreten Fall ging es um die Durchführung so genannter Plausibilitätsprüfungen, die in § 106 a SGB V geregelt sind. Damit diese Prüfungen sachgerecht durchgeführt werden können, bestimmt § 295 Abs. 1 a SGB V, dass die an der vertragsärztlichen Versorgung teilnehmenden Ärzte verpflichtet und befugt sind, auf Verlangen der Kassenärztlichen Vereinigungen die für die Prüfung erforderlichen Befunde vorzulegen.

Ich habe deshalb den anfragenden Ärzten mitgeteilt, dass sie keine Befürchtungen in Bezug auf eine Verletzung ihrer ärztlichen Schweigepflicht haben müssen, wenn sie die geforderten Unterlagen vorlegen.

10 Forschung

10.1 Einführung eines Forschungsgeheimnisses für medizinische Daten

Bei vielen medizinischen Forschungsvorhaben benötigen Forscherinnen und Forscher Patientendaten für ihre Arbeit. Die Datenschutzbeauftragten des Bundes und der Länder halten es für unbefriedigend, dass nach der jetzigen Rechtslage die Daten dabei den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren verlieren.
In einer Entschließung (siehe Anlage 15.20) hat sich die Konferenz der Datenschutzbeauftragten auf ihrer Tagung am 25./26. März 2004 für die Einführung eines Forschungsgeheimnisses für medizinische Daten ausgesprochen.

10.2 MRSA-Prävalenzstudie in Alten- und Pflegeheimen

Im Berichtszeitraum wurde ich über eine Studie des Instituts für Medizinische Mikrobiologie und Hygiene der Universitätskliniken des Saarlandes zur Häufigkeit des Auftretens bestimmter bakterieller Krankheitserreger in Alten- und Pflegeheimen informiert. Es handelt sich um sogenannte MRSA-Bakterien (Methicillin-resistente Staphylococcus aureus), die bei Personen, die sich einer Operation oder einer Krankenhausbehandlung unterziehen müssen, zu einer Infektion führen können.
Ziel der Untersuchung war die Feststellung der derzeitigen „MRSA-Situation“ in den Einrichtungen im Saarland, der Vergleich der verschiedenen Einrichtungen untereinander, gegebenenfalls das Aufzeigen von MRSA-Häufungen sowie das Erarbeiten spezieller Problemlösungen betroffener Einrichtungen.
Von Seiten des Instituts war man der Auffassung, dass „keine datenschutzrechtlichen Probleme bestehen sollten“, da die Erhebung und Auswertung der Daten zum Zwecke der Veröffentlichung anonymisiert erfolge. So war es zu erklären, dass die Einholung einer Einverständniserklärung in die Erhebung und Verarbeitung der für die Durchführung der Studie benötigten Daten nicht vorgesehen war.

Auch wenn die weitere Verarbeitung der Daten in anonymisierter Form erfolgen sollte, so handelte es sich doch um eine personenbezogene Datenerhebung, die mangels Vorliegens einer gesetzlichen Rechtsgrundlage nur zulässig war mit dem Einverständnis der betroffenen Heimbewohnerinnen und Heimbewohner. Neben der Entnahme eines Nasenabstrichs sollte auch noch nach vorhandenen Begleiterkrankungen, Vorerkrankungen und früheren Krankenhausaufenthalten gefragt werden. Außerdem sollte der Befund der Leitung des Pflegeheimes mitgeteilt werden, die ihrerseits wiederum den Hausarzt der Betreffenden informieren sollte. Auch bei diesem Vorgang handelt es sich um eine personenbezogene Datenverarbeitung, die nur zulässig ist mit dem Einverständnis der Betroffenen.

Das Institut hat auf meine Anregung hin eine Einverständniserklärung formuliert, in der die Betroffenen über die Ziele der Studie und die beabsichtigte Verarbeitung ihrer personenbezogenen Daten im Einzelnen informiert wurden. Ganz wichtig war in diesem Zusammenhang der Hinweis auf die Freiwilligkeit der Teilnahme an der Studie, der auf meinen Vorschlag hin noch eingearbeitet wurde.

Im Ergebnis kann ich feststellen, dass die konstruktive Zusammenarbeit letztlich zu einer datenschutzgerechten Ausgestaltung der Studie geführt hat.

11 Schulen

11.1 Chipkarte für Studierende

Zum Wintersemester 2004/2005 hat die Universität des Saarlandes den Studierendenausweis in Form einer multifunktionellen Chipkarte eingeführt. Folgende Funktionen sind bisher nutzbar: Studierendenausweis, Bedienstetenausweis, Semesterticket, Geldbörse mit Zahlungsfunktion für die Mensa und Cafeterien des Studentenwerks, Ausweis für die Bibliotheksnutzung, Identifikation gegenüber Zutrittskontrollsystemen, Identifikation bei der Einfahrtskontrolle sowie Zeiterfassung für Bedienstete der zentralen Verwaltung und der saarländischen Universitäts- und Landesbibliothek. In Vorbereitung sind weitere Teilfunktionen an verschiedenen Stellen der Universität wie beispielsweise Fernleih- und Säumnisgebühren der Bibliothek, Nutzung und Bezahlung bei zentralen Druckausgaben, bei der Parkhausbewirtschaftung und weiterer Verwaltungsgebühren. Ferner sollen später die Rückmeldefunktionen, Adressänderungen und der Bescheinigungsdruck an Infoterminals auf dem Campus ermöglicht werden. Nachdem es anfänglich zu Irritationen zwischen meiner Dienststelle und der Universität wegen meiner Beteiligung bei Einführung der Karte gegeben hatte, entwickelte sich in der Folge eine konstruktive Zusammenarbeit, die letztlich dazu geführt hat, dass die datenschutzrechtlichen Aspekte ausreichend Beachtung gefunden haben. Zu nennen sind hier insbesondere folgende Gesichtspunkte:

- Die Chipkarte wird nicht als Datenträger für personenbezogene Informationen eingesetzt. Auf der Karte aufgedruckt sind lediglich die Bezeichnung „Studierendenausweis“ oder „Gasthörerausweis“, Kartenseriennummer, Passbild, Vorname, Name, Titel, Matrikelnummer.
- Auf dem Chip befinden sich 16 Sektoren, die von den einzelnen Hintergrundsystemen genutzt werden können. Diese sind nur über einen separaten Schlüssel ansprechbar und gegeneinander abgeschottet. In jedem Sektor sind nur diejenigen Informationen gespeichert, die für die jeweiligen Anwendungen wie z.B. die elektronische Börse oder die Anbindung an die Bibliothek tatsächlich erforderlich sind. Dadurch ist sichergestellt, dass durch die Chipkarte keine Verknüpfungen zwischen diesen Hintergrundsystemen hergestellt werden können.

- Jeder Chipkarteninhaber kann sich seine auf der Karte und im Kartenmanagementsystem gespeicherten Daten im Kartenbüro anzeigen lassen.
- Die Universität hat ein Merkblatt zu der Chipkarte herausgegeben, in dem die Studierenden umfassend über die Funktionalitäten der Karte, aber auch über die dabei stattfindenden Datenverarbeitungsvorgänge sowie die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung der zu ihrer Person gespeicherten Daten nach Maßgabe der Vorschriften des saarländischen Datenschutzgesetzes informiert werden.

11.2 Datenabgleich beim BAföG mit dem Bundesamt für Finanzen

In meinem letzten Tätigkeitsbericht (19. TB 2001/2002, TZ 10.1) habe ich über den Datenabgleich der BAföG-Ämter mit dem Bundesamt für Finanzen berichtet, mit dessen Hilfe falsche Vermögensangaben der BAföG-Antragsteller aufgedeckt werden sollten. Ich habe die Verfahrensweise in den anderen Bundesländern als datenschutzrechtlich unzulässig kritisiert, weil eine entsprechende Befugnisnorm für die Übermittlung von Sozialdaten von den BAföG-Ämtern an das Bundesamt für Finanzen fehlte.
Ich möchte berichten, wie es im Saarland weiterging: Stand bei Redaktionsschluss meines letzten Tätigkeitsberichtes noch nicht fest, ob sich auch das Saarland an dem Abgleichverfahren beteiligt, so wurde der Abgleich mittlerweile auch im Saarland durchgeführt. Auch hier wurde eine Vielzahl von Fällen festgestellt, in denen Studenten ihrer Bank Freistellungsaufträge erteilt hatten. Diese Fälle wurden überprüft, es wurden Rückforderungsbescheide erlassen und es kam zu Anzeigen bei der Staatsanwaltschaft.

Mittlerweile ist seit 8. Dezember 2004 eine Regelung im Bundesausbildungsförderungsgesetz in Kraft (§ 41 Abs. 4 BAföG), die den fraglichen Datenabgleich erlaubt. Nach dieser Vorschrift dürfen die Ämter für Ausbildungsförderung Personen, die Leistungen nach dem BAföG beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs darauf hin überprüfen, ob und welche Daten nach § 45 d Abs. 1 des Einkommensteuergesetzes dem Bundesamt für Finanzen übermittelt worden sind. Die Ämter für Ausbildungsförderung dürfen zu diesem Zweck Namen, Vorna-

men, Geburtsdatum und Anschrift der Personen, die Leistungen nach dem BAföG beziehen, dem Bundesamt für Finanzen übermitteln. Das Bundesamt für Finanzen hat die ihm überlassenen Daten und Datenträger nach Durchführung des Abgleichs unverzüglich zurückzugeben, zu löschen oder zu vernichten. Die übermittelten Daten der Personen, bei denen die Überprüfung zu keinen abweichenden Feststellungen geführt hat, sind unverzüglich zu löschen.

11.3 EDV-Programm „Schulverwaltung Grundschule“

Das Ministerium für Bildung, Kultur und Wissenschaft hat mir die Verfahrensdokumentation für ein einheitliches Schulverwaltungsprogramm Grundschule zur datenschutzrechtlichen Beurteilung vorgelegt. So begrüßenswert dieses Vorhaben auch ist, muss es sich doch an den vorgegebenen rechtlichen Rahmen der Datenverarbeitung halten. Der Datensatz enthält mehrere Felder, für die nach den geltenden Bestimmungen keine Rechtsgrundlage vorhanden ist, z.B. die automatisierte Verarbeitung von Daten wie Linkshänder, Sehbehinderung, Hörbeeinträchtigung, Sprachbeeinträchtigung, Asylbewerber, Migrationsstatus, Religionswunsch. Die vom Kultusministerium 1986 erlassene Rechtsverordnung über die Verarbeitung personenbezogener Daten in den Schulen regelt in einem Maximalkatalog, welche Daten der Schüler und Erziehungsberechtigten in den einzelnen Schulformen verarbeitet werden dürfen. Zusätzlich bestimmt § 5 dieser Verordnung, dass Gesundheitsdaten nicht automatisiert verarbeitet werden dürfen.
Der Landesbeauftragte für Datenschutz hat mehrmals auf die Notwendigkeit hingewiesen, diese Rechtsverordnung zu überarbeiten. Abgesehen von einzelnen Korrekturen, zuletzt bei der Einfügung des § 5 a wegen des Einsatzes privater PC von Lehrkräften, sind bisher umfassende Änderungen der Verordnung nicht erfolgt. Eventuelle Anforderungen der Statistik können die Datenverarbeitung in dem vorgesehenen Umfang ebenfalls nicht rechtfertigen, weil auch die Schulstatistikverordnung in der geltenden Fassung hierfür keine Rechtsgrundlage bietet. Ich konnte daher aus datenschutzrechtlicher Sicht der Freigabe des Programms nicht zustimmen.

11.4 Novellierung des Universitätsgesetzes

Im Berichtszeitraum wurde das saarländische Universitätsgesetz geändert. Ich hatte Gelegenheit, zu dem Gesetzentwurf aus datenschutzrechtlicher Sicht Stellung zu nehmen.

In meiner Stellungnahme habe ich ausgeführt, dass die Novellierung ein guter Anlass sei, insbesondere zwei grundsätzliche Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten im Universitätsbereich detaillierter, als im Entwurf vorgesehen, zu regeln: Die Evaluierung von Leistungen der Universität in Forschung und Lehre sowie datenschutzrechtliche Fragen im Zusammenhang mit der Einführung eines maschinenlesbaren Studierendenausweises.

Im Zusammenhang mit der Bewertung der Qualität der Arbeit der Hochschulen stellt sich aus datenschutzrechtlicher Sicht die Problematik, in welchem Umfang in diesem Zusammenhang personenbezogene Daten der Studierenden und der betroffenen Professoren verarbeitet werden dürfen. Im Rahmen der Novellierung hätte Gelegenheit bestanden, in diesem Punkt Klarheit durch eine entsprechende normenklare Formulierung herbeizuführen. Den von mir unterbreiteten Formulierungsvorschlag hat der Gesetzgeber leider nicht aufgegriffen. Immerhin verpflichtet das am 27. August 2004 in Kraft getretene Universitätsgesetz die Universität, in einer Ordnung Bestimmungen über die Bewertungsverfahren und über die Veröffentlichung der daraus gewonnenen Ergebnisse zu treffen. Mir ist nicht bekannt, wie der Verfahrensstand im Hinblick auf den Erlass dieser Ordnung ist.

Grundsätzlich begrüßt habe ich die Schaffung einer Rechtsgrundlage für die Einführung des beabsichtigten maschinenlesbaren Studierendenausweises. Ich habe in diesem Zusammenhang eine klarstellende Formulierung vorgeschlagen, dass der Studienausweis auch in Form eines mobilen personenbezogenen Datenverarbeitungssystems (Chipkarte) ausgegeben werden kann und dass die näheren Einzelheiten, insbesondere die möglichen Funktionen der Chipkarte, in einer Ordnung geregelt werden. Auch hier fehlen mir Informationen über den Stand der Arbeiten zum Erlass dieser Ordnung; die Chipkarte ist seit dem Wintersemester 2004/2005 an der

Universität des Saarlandes eingeführt. Das Thema „Chipkarte“ ist Gegenstand der Textziffer 11.1 dieses Tätigkeitsberichtes.

Entschieden habe ich mich gegen die vorgesehene Regelung gewandt, zukünftig auch Daten ehemaliger Studierender, insbesondere zum beruflichen Werdegang, zu erheben und zu bearbeiten. Ich habe darauf hingewiesen, dass ich hier einen besonders intensiven Eingriff in das Recht auf informationelle Selbstbestimmung sehe, weil es sich bei Darstellung des Berufslebens einer Person um besonders sensible Daten handelt. Eine zentrale personenbezogene Speicherung ist für mich ein unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, zumal sich mir die Geeignetheit und Erforderlichkeit eines solchen Registers nicht ohne weiteres erschließen. Leider wurde meinen Bedenken auch in diesem Punkt nicht Rechnung getragen.

11.5 Unterschriftenaktion im Schulgottesdienst

Eine Mutter wandte sich empört an meine Dienststelle und schilderte folgenden Sachverhalt:
Ihre beiden Kinder im Alter von 11 und 14 Jahren hatten an einem katholischen Schulgottesdienst teilgenommen. Während des Gottesdienstes wurden an die Kinder „Postkarten“ des Misereor-Hilfswerkes verteilt, die von den Kindern zu unterschreiben und mit einem Fingerabdruck zu versehen waren. Mit dem Fingerabdruck sollte die Unterstützung „besiegelt“ werden. Die Kinder sollten Ihre Unterschrift unter folgenden Text setzen:
„Ich fordere die Bundesregierung dazu auf, im Rahmen der Welthandelsorganisation (WTO) dafür zu sorgen, dass

- die Patentierung von Saatgut, Pflanzen und Tieren sowie deren Teilen und Genen ausgeschlossen wird,
- die WTO-Ministerkonferenz eindeutig erklärt, dass nichts im TRIPs-Abkommen so ausgelegt werden darf, dass es die Ernährungssicherheit und die biologische Vielfalt gefährden kann,
- die WTO die Konvention über die biologische Vielfalt anerkennt, insbesondere die in der Konvention verankerten Bauernrechte und Verbote von Biopiraterie.“

In diesem Fall war zunächst zu klären, wer die zuständige Datenschutzkontrollinstanz für das Anliegen der Petentin war (meine Dienststelle oder der Datenschutzbeauftragte der katholischen Kirche). Ich bin zu dem Ergebnis gekommen, dass es sich bei dem fraglichen Schulgottesdienst zumindest auch um eine schulische Veranstaltung gehandelt hat. Voraussetzung für eine Zuständigkeit meiner Dienststelle wäre jedoch gewesen, dass die Schule personenbezogene Daten der Schüler erhoben hätte. Nach Aussage des Schuldirektors war die Schule nicht in die Vorbereitung des Gottesdienstes einbezogen; die Verantwortung für die Gestaltung des Schulgottesdienstes lag vielmehr allein bei der Kirche. Ich habe den Vorgang dem Datenschutzbeauftragten der katholischen Kirche zur weiteren Bearbeitung abgegeben. Gegenüber der Petentin habe ich zum Ausdruck gebracht, dass ich den Vorgang für äußerst bedenklich halte, weil hier minderjährige Kinder, die die Tragweite ihrer Erklärung nicht abschätzen konnten und wohl zusätzlich unter faktischem Druck standen, veranlasst wurden, ihre Unterschriften zu leisten.

Der Datenschutzbeauftragte der katholischen Kirche hat dies genauso gesehen und die Erhebung der Daten ohne Einwilligung der Erziehungsberechtigten als unzulässig bezeichnet.

12 Öffentlicher Dienst

12.1 Information über einzelne Beteiligungsvorgänge durch den Personalrat in der Personalversammlung

Nach dem Saarländischen Personalvertretungsgesetz (§ 48 SPersVG) hat der Personalrat einmal in jedem Kalenderhalbjahr in einer Personalversammlung einen Tätigkeitsbericht zu erstatten. Keine Probleme aus datenschutzrechtlicher Sicht können entstehen, soweit der Personalrat über allgemeine Tarif-, Sozial- oder Organisationsfragen in der Dienststelle berichtet. Anders sieht es dagegen aus, wenn es um Darstellung der Mitwirkung des Personalrates bei Beteiligungsfällen geht, z.B. Einstellungen, Beförderungen oder Entlassungen. Hier kann es zu einem Konflikt kommen zwischen der umfassenden Berichtspflicht des Personalrates auf der einen Seite und den Persönlichkeitsrechten der von der Darstellung im Tätigkeitsbericht des Personalrates betroffenen Bediensteten.

So hat sich ein Mitarbeiter einer Behörde bei meiner Dienststelle darüber beschwert, dass in einem Tätigkeitsbericht über die Vorgehensweise des Personalrates in seiner ganz konkreten Beförderungsangelegenheit berichtet worden sei. Ein Rückschluss auf seine Person sei aufgrund der mitgeteilten Informationen für jeden Mitarbeiter der Behörde möglich gewesen.
Sicher ist es für die Beurteilung der Effektivität der Arbeit eines Personalrates interessant zu erfahren, wie dieser insbesondere in Fällen agiert, in denen es zu Differenzen zwischen der Dienststellenleitung und dem Personalrat kommt. Diesem Interesse stehen allerdings die Persönlichkeitsrechte der von der Darstellung betroffenen Mitarbeiter entgegen.
Im Ergebnis bin ich der Auffassung, dass der Personalrat seine Pflicht, die Personalversammlung umfassend über seine Tätigkeit zu informieren, auch erfüllen kann, ohne dass einzelne Beteiligungsfälle im Detail geschildert werden. Im Zweifelsfall haben jedenfalls die Persönlichkeitsrechte der Mitarbeiter und das Recht auf Schutz ihrer Personaldaten Vorrang vor einer Information aller übrigen Mitarbeiter der Dienststelle über sie betreffende Personalangelegenheiten.

Meine Auffassung wird gestützt durch eine Vorschrift im Saarländischen Personalvertretungsgesetz (§ 9 SPersVG), wonach Personalratsmitglieder über ihnen im Rahmen ihrer Tätigkeit bekannt gewordene Angelegenheiten und Tatsachen Stillschweigen zu bewahren haben. Die teilweise in der Literatur zu dieser Vorschrift vertretene Auffassung, die Teilnehmer der Personalversammlung dürften auch über Angelegenheiten informiert werden, die Außenstehenden gegenüber der Geheimhaltung bedürfen (da die Teilnehmer an der Personalversammlung ihrerseits der Schweigepflicht unterliegen) kann ich – jedenfalls soweit es um Personaldaten geht – nicht teilen. Denn damit würde der Personaldatenschutz innerhalb einer Dienststelle praktisch außer Kraft gesetzt.

12.2 Dienstbezeichnung der Lehrkräfte auf Schulzeugnissen

Mehrere Lehrer hatten sich an mich gewandt, weil sie durch die vorgeschriebenen Formulare genötigt waren, in den Abschlusszeugnissen die Dienstbezeichnung anzugeben. Sie sahen sich dadurch in ihrem Persönlichkeitsrecht beeinträchtigt. Ein Lehrer erläuterte seine Situation. Wegen des Beförderungsstaus sei er nach fast 30jähriger Dienstzeit trotz ausgezeichneter Beurteilungen noch nie befördert worden. Die Öffentlichkeit könne denken, dass ein Lehrer in diesem Alter sich etwas zu Schulden kommen ließ oder ein schlechter Lehrer sei, wenn er noch immer im Eingangsamt „verharre“. Das Ministerium für Bildung, Kultur und Wissenschaft teilte mir in seiner Stellungnahme mit, dass die einschlägigen Schulordnungen überwiegend für die Unterzeichnung von Zeugnissen nur Funktionsangaben wie Klassenleiter, Schulleiter oder Vorsitzender der Prüfungskommission vorschreiben. Aus schulischer Sicht werde die Angabe von Amtsbezeichnungen auf den Zeugnissen nicht für notwendig gehalten.

Nach den Bestimmungen des Personalaktenrechts dürfen Name und Amtsbezeichnung von Beamten an Dritte nur übermittelt werden, soweit es der Dienstverkehr erfordert (§ 108 d Abs. 2 Satz 3 Saarländisches Beamtengesetz). Ich kann nicht erkennen, dass die Angabe der Dienst- oder Amtsbezeichnung in einem Zeugnis im datenschutzrechtlichen Sinne erforderlich ist. Nach meiner Auffassung reicht es aus, wenn die Funktion des jeweiligen Lehrers angegeben wird.

12.3 Meldung der Arbeitsunfähigkeit von Angestellten an die Zentrale Besoldungs- und Versorgungsstelle

In einem Schreiben mit der Überschrift „Verfahren im Zusammenhang mit der Meldung der Arbeitsunfähigkeit von Angestellten an die Zentrale Besoldungs- und Versorgungsstelle“ forderte das Landesamt für Finanzen alle obersten Landesbehörden im Saarland dazu auf, „anlässlich der Fehlzeitengespräche zu eruieren, welche Krankheit zu der Arbeitsunfähigkeit geführt hat und – soweit bekannt – die Art der Erkrankung auf einem Meldeformular anzugeben“.
Ich halte es für datenschutzrechtlich nicht zulässig, dass der Arbeitgeber bei Arbeitsunfähigkeit nach der Art der jeweiligen Erkrankung fragt; diese Frage muss von dem Bediensteten nicht beantwortet werden. Denn eine Rechtsgrundlage für eine solche Datenerhebung ist nicht ersichtlich.
Soweit der Arbeitgeber beurteilen muss, ob Arbeitsunfähigkeitszeiten die gleiche Krankheit zugrunde liegt (dies ist von Bedeutung für die Dauer des Krankengeldanspruches), kann er sich an die Krankenkasse des Bediensteten wenden. Gemäß § 69 Abs. 4 SGB X sind die Krankenkassen befugt einem Arbeitgeber mitzuteilen, ob die Fortdauer einer Arbeitsunfähigkeit oder eine erneute Arbeitsunfähigkeit eines Arbeitsnehmers auf derselben Krankheit beruht, wobei die Übermittlung von Diagnosen an den Arbeitgeber nicht zulässig ist.

Ich habe meine Rechtsauffassung allen obersten Landesbehörden mitgeteilt und gebeten, bei Arbeitsunfähigkeit von Fragen nach der Art der Erkrankung Abstand zu nehmen.

Nachdem zunächst keine Reaktion auf meinen Hinweis erfolgte, wurde mir dann doch der Entwurf eines Erlasses des damaligen Ministeriums für Finanzen und Bundesangelegenheiten zum Meldeverfahren bei Arbeitsunfähigkeit von Angestellten vorgelegt. Meinen datenschutzrechtlichen Bedenken war Rechnung getragen worden; eine Meldung der Art der Erkrankung war in dem Erlassentwurf nicht mehr vorgesehen.

12.4 Mitarbeiterdaten im Intranet einer Stadt

Der Datenschutzbeauftragte einer saarländischen Stadt wollte meine Auffassung zu der Absicht der dortigen Personalabteilung wissen, im Intranet eine Personalübersicht über alle städtischen Bediensteten zu erstellen. Geplant war, Namen, Anschrift, Telefonnummern (dienstlich, privat, Handy), die Organisationseinheit, bei der/die Bedienstete beschäftigt ist, sowie ein Lichtbild in das Intranet einzustellen.

Ausgangspunkt der datenschutzrechtlichen Beurteilung ist die Vorschrift des § 4 Abs. 1 Saarländisches Datenschutzgesetz, wonach eine Verarbeitung personenbezogener Daten nur zulässig ist, wenn entweder das saarländische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.
Die Zulässigkeit der Verarbeitung von Mitarbeiterdaten ist in § 31 SDSG geregelt, wonach Daten von Beschäftigten verarbeitet werden dürfen, wenn dies zur Durchführung des Dienst- oder Arbeitsverhältnisses erforderlich ist.
Für einen Teil der Daten kann die beabsichtigte Verarbeitung auf diese Vorschrift gestützt werden. Das sind die Angaben, die üblicherweise in Organisationsplänen der Verwaltung enthalten sind, weil sie für die dienstliche Erreichbarkeit erforderlich sind, nämlich Name, dienstliche Telefonnummer sowie die Organisationseinheit.
Die Erforderlichkeit der Einstellung von Lichtbildern aller Bediensteten im Intranet kann ich dagegen nicht nachvollziehen. Wenn hier als Begründung genannt wird, dass dies dem besseren und schnelleren Kennenlernen von Auszubildenden oder neu eingestellten Mitarbeitern dienen soll, kann ich mich des Eindrucks nicht erwehren, dass hier die Möglichkeiten der neuen Technik genutzt werden sollen, ohne die Erforderlichkeit der Datenverarbeitung an dem strengen Grundsatz der Erforderlichkeit zu messen.
Auch der für die Bekanntgabe der privaten Telefon- und Handynummern genannte Grund, Mitarbeiter außerhalb der Arbeitszeit im Bedarfsfall heranziehen zu können, kann es nicht rechtfertigen, diese Daten allen anderen Bediensteten zur Kenntnis zu bringen. Hinzu kommt, dass wohl nicht alle Mitarbeiter außerhalb der Arbeitszeiten jederzeit erreichbar sein müssen.

Ich meine, dass die Einstellung der Daten in das Intranet auch nicht auf die Einwilligung der Mitarbeiter gestützt werden kann. Für den Zweck „Erreichbarkeit außerhalb der Arbeitszeiten“ ist die Einholung von Einwilligungen nicht geeignet. Eine Einwilligung darf auch verweigert werden, so dass die Daten dieser Mitarbeiter nicht ins Intranet gestellt werden dürften, ein Ergebnis, das aus Sicht der Stadtverwaltung nicht befriedigen kann.
Was die Veröffentlichung der Lichtbilder auf der Grundlage der Einwilligung angeht, habe ich doch erhebliche Zweifel, ob hier die Freiwilligkeit der Einwilligung wegen des damit verbundenen faktischen Zwanges gewährleistet ist.

Ich möchte alle Behörden und öffentlichen Institutionen an ihre Verpflichtung erinnern, bei Erstellung eines Intranet-Angebotes genau zu prüfen, ob alle Daten wirklich für den Ablauf eines ordnungsgemäßen Dienstbetriebes erforderlich sind.

12.5 Richtlinie zur Einführung von Telearbeit in der Landesverwaltung

Die Landesregierung hat es sich zum Ziel gesetzt, ihren Bediensteten in verstärktem Maße die Möglichkeit der Telearbeit anzubieten. Mit dieser Arbeitsform soll die Vereinbarkeit von Beruf und persönlicher Lebenssituation, insbesondere der Kinderbetreuung, sowie die Arbeitszufriedenheit insgesamt gefördert werden. Unter dem Begriff Telearbeit werden alle Formen von Tätigkeiten erfasst, die mittels Informations- und Kommunikationstechnologien mit gewisser Regelmäßigkeit außerhalb der Dienststelle auf einem häuslichen Arbeitsplatz erbracht werden.
Unter Federführung des Ministeriums für Inneres und Sport wurde eine Projektgruppe eingerichtet, die eine landeseinheitliche Richtlinie für die Einführung von Telearbeit erstellen sollte. In dieser Richtlinie sollten alle Aspekte, die bei der Einrichtung von Telearbeitsplätzen eine Rolle spielen, zusammengefasst werden. Auch Mitarbeiter meiner Dienststelle waren zu den Projektgruppensitzungen eingeladen, denn wenn im Rahmen der Telearbeit personenbezogene Daten verarbeitet werden, sind naturgemäß auch Datenschutzbelange berührt. Es geht hier insbesondere darum, die Gefahren zu minimieren, die aus der Tatsache entstehen, dass personenbezogene Daten das dienstliche Umfeld verlassen. Man denke nur an den Transport der

Daten von der Dienststelle zu der eigenen Wohnung oder die Möglichkeit des Zugangs von Familienmitgliedern oder sonstigen Personen zu vertraulichen Informationen.

Um die hierbei entstehenden Risiken möglichst auszuschließen, muss sich der Bedienstete nach der am 1. August 2004 in Kraft getretenen „Richtlinie zur Einführung von Telearbeit in der saarländischen Landesverwaltung“ verpflichten,

- für die Einhaltung der Bestimmungen des saarländischen Datenschutzgesetzes und der im Zusammenhang mit Geheimhaltungspflichten zu beachtenden sonstigen Schutzvorschriften zu sorgen,
- den Arbeitsplatz in einem separaten, abschließbaren Arbeitszimmer in der Wohnung einzurichten,
- eigenverantwortlich für den datenschutzsicheren Transport und die Unterbringung der Arbeitsunterlagen in abschließbaren Containern oder Schränken zu sorgen,
- die Vernichtung von Schriftgut und sonstigen Datenträgern datenschutzgerecht vorzunehmen,
- dafür zu sorgen, dass Dritte keinen Zugang zu den geschützten Daten haben,
- nur die zur Verfügung gestellten Geräte (Hard- und Software) zu nutzen und keine Veränderungen vorzunehmen,
- die zur Verfügung gestellten Arbeitsmittel nicht privat zu nutzen,
- Vorkommnisse, welche die Sicherheit der geschützten Daten und die Geheimhaltungspflichten betreffen, der Dienststelle unverzüglich zu melden.

Darüber hinaus muss der Bedienstete eine Erklärung unterschreiben, dass er damit einverstanden ist, dass der Landesbeauftragte für Datenschutz – auch ohne Voranmeldung – Zugang zu seinem häuslichen Arbeitsplatz hat, um die Einhaltung der Datenschutzvorschriften zu kontrollieren. Wichtig ist schließlich auch die Bestimmung in der Richtlinie, wonach bei einer beabsichtigten Verarbeitung besonders sensibler personenbezogener Daten eine Einzelfallprüfung durch den Landesbeauftragten für Datenschutz erfolgt.

Ich habe mir vorgenommen, die Einhaltung der Vorschriften der Richtlinie vor Ort zu überprüfen. Über die Ergebnisse werde ich in meinem nächsten Tätigkeitsbericht berichten.

13 Rundfunk und Medien, Telekommunikation

13.1 EU-Rahmenbeschluss zur Vorratsspeicherung in der Telekommunikation

Nach intensiven Diskussionen hat sich der Bundesgesetzgeber im Rahmen der Novellierung des Telekommunikationsgesetzes dafür entschieden, dass bei der Telekommunikation anfallende Verkehrsdaten nicht auf Vorrat für Strafverfolgungszwecke gespeichert werden dürfen. Gerade in die gegenteilige Richtung läuft ein Rahmenbeschluss von 4 EU-Mitgliedsstaaten, nämlich Frankreich, Irland, Schweden und Großbritannien, wonach eine umfassende Speicherung von Kommunikationsdaten für Zwecke der Strafverfolgung zulässig sein soll. Der Entwurf sieht eine Mindestspeicherfrist von 12 bis zu 36 Monaten vor. Gespeichert werden sollen alle Verkehrsdaten der Telekommunikation im Fest- und Mobilfunk. Gleiches soll auch für SMS-Kurzmitteilungen und Internet-Kommunikation über eMail, aber auch z.B. für Protokolle über Internetzugriffe gelten.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen solche Pläne zur Vorratsdatenspeicherung und haben sich zu den Bestrebungen auf EU-Ebene in einer gemeinsamen Presserklärung wie folgt geäußert:
„Der Bundesgesetzgeber hat erst vor kurzem bei der Verabschiedung des neuen Telekommunikationsgesetzes aus gutem Grund die Einführung einer Pflicht zur Vorratsdatenspeicherung abgelehnt. Das grundgesetzlich garantierte Fernmeldegeheimnis lässt eine Speicherung von Daten über die Nutzung öffentlicher Telekommunikationsnetze (insbesondere auch des Internets) außer für betriebliche Zwecke nur zu, wenn ein konkreter Verdacht für eine Straftat von erheblicher Bedeutung besteht.

Zudem würde eine flächendeckende Vorratspeicherung von Kommunikationsdaten auch die Grundrechte auf freie Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen verletzen. Jede Auswertung von Internetadressen kann etwas über die Interessen, Vorlieben und politischen Präferenzen der

Nutzenden verraten. Diese Adressen müssten nach dem Vorschlag für einen Rahmenbeschluss auf Vorrat gespeichert werden.

Darüber hinaus bestehen erhebliche Zweifel, ob der vorgeschlagene Rahmenbeschluss mit Artikel 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung des Privatlebens und der Korrespondenz) vereinbar ist. Der Europäische Gerichtshof für Menschenrechte hat betont, dass die Vertragsstaaten auch zur Bekämpfung des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten. Vielmehr muss es sich um Maßnahmen handeln, die in einer demokratischen Gesellschaft notwendig sind und dem Verhältnismäßigkeitsgrundsatz entsprechen. Die flächendeckende anlassunabhängige Speicherung aller Daten über die Nutzung öffentlicher Kommunikationsnetze schießt dagegen weit über das für die Vorbeugung und Verfolgung von Straftaten erforderliche Maß hinaus.

Die Datenschutzbeauftragten fordern die Bundesregierung auf, den Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten über die Nutzung von öffentlichen elektronischen Kommunikationsdiensten und –netzen abzulehnen."

13.2 GEZ-Online

Für die Bearbeitung der Anträge auf Befreiung von der Rundfunkgebührenpflicht setzen die saarländischen Gemeinden und Städte neuerdings ein automatisiertes Verfahren ein. Damit können die erforderlichen Daten bei den Sozialämtern am PC erfasst und auf elektronischen Datenträgern verschlüsselt der Gebühreneinzugszentrale (GEZ) übermittelt werden. Aus datenschutzrechtlicher Sicht bestehen gegen das Verfahren keine durchgreifenden Bedenken. Ich habe allerdings Wert darauf gelegt, dass eine automatisierte Import-/Export-Schnittstelle zum Sozialhilfe-Verfahren nicht eingerichtet wird. Werden Anträge auch bei den Bürgerämtern entgegengenommen, darf dort kein Zugriff zum automatisierten Sozialhilfebestand möglich sein; hierfür ist im Sozialgesetzbuch keine Rechtsgrundlage vorhanden (vgl. § 79 SGB X).

13.3 Novellierung des Telekommunikationsgesetzes

Im Berichtszeitraum wurde das Telekommunikationsgesetz vor dem Hintergrund der Umsetzung verschiedener europäischer Richtlinien umfassend novelliert. Auch die Datenschutzregelungen waren von der Neuordnung betroffen.
Zu erwähnen ist, dass gesetzestechnisch die bisherigen Regelungen der Telekommunikations-Datenschutzverordnung (TDSV) in das Telekommunikationsgesetz integriert worden sind. Inhaltlich hat das Gesetz Verschlechterungen für den Datenschutz mit sich gebracht. Die Verkehrsdaten dürfen nunmehr bis zu 6 Monaten nach Versendung der Rechnung gespeichert werden. Bisher war es so, dass diese Daten grundsätzlich nur unter Kürzung der Zielnummer um die letzten 3 Ziffern für diesen Zeitraum gespeichert wurden. Nur wenn der Kunde es ausdrücklich verlangte, durften die Daten vollständig gespeichert werden. Dieses Regel-Ausnahmeverhältnis wurde im neuen Telekommunikationsgesetz umgekehrt; der Teilnehmer muss von sich aus aktiv werden, um die Kürzung der Zielnummer um die letzten 3 Ziffern zu erreichen. In einer Entschließung vom 21. November 2003 (s. Anlage 15.14) hatten die Datenschutzbeauftragten des Bundes und der Länder diese Absichten der Bundesregierung wegen erheblicher verfassungsrechtlicher Bedenken kritisiert. Die Datenschutzbeauftragten haben moniert, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für Abrechnungszwecke nicht mehr benötigen. Leider konnten sich die Datenschutzbeauftragten mit ihren Vorbehalten im weiteren Gesetzgebungsverfahren nicht durchsetzen; verhindert werden konnte allerdings wenigstens die Forderung des Bundesrates, die Anbieter allein im Interesse der Sicherheitsbehörden zu einer 6-monatigen Speicherung aller Verkehrsdaten zu verpflichten.

In ihrer o.a. Entschließung hatten sich die Datenschutzbeauftragten zudem gegen die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys gewandt, weil sie zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und es ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden. Auch in diesem

Punkt hat sich der Gesetzgeber für eine weitere Aushöhlung des grundrechtlich geschützten Fernmeldegeheimnisses entschieden; eine anonyme Handy-Karte wird es nicht mehr geben.

13.4 Übermittlung personenbezogener Daten an die Medien

Nach den Mediengesetzen haben Behörden den Vertreterinnen und Vertretern der Medien Auskünfte zu erteilen, die der Erfüllung der öffentlichen Aufgabe der Medien dienen (vgl. § 5 Saarländisches Mediengesetz, SMG).

Beinhalten diese Informationen personenbezogene Daten, so können die Auskünfte unter bestimmten Voraussetzungen verweigert werden. Es können Vorschriften über die Geheimhaltung und auch besondere Berufs- oder Amtsgeheimnisse, wie beispielsweise das Steuer- oder Sozialgeheimnis, entgegenstehen. Auch wenn ein überwiegendes öffentliches oder schutzwürdiges privates Interesse verletzt würde, kann die Auskunft an die Medien verweigert werden (§ 5 Abs. 2 Nr. 3 SMG). Gegenstand des schutzwürdigen privaten Interesses ist hier vor allem das Recht auf informationelle Selbstbestimmung, das unter anderem im Recht am eigenen Bild zum Ausdruck kommt.

Mit welchen Schwierigkeiten die eigenen notwendigen Ermessensentscheidungen der Medien bei der Erfüllung ihrer öffentlichen Aufgabe und bei der Abwägung zwischen den Persönlichkeitsrechten und dem Informationsinteresse der Öffentlichkeit verbunden sind, zeigten sehr deutlich die Entscheidungen der Gerichte in den sogenannten „Caroline von Monaco“-Urteilen (BVerfG, NJW 2000, 1021; EGMR, NJW 2004, 2647).
Die Behörden haben neben der Entscheidung, ob überhaupt Auskunft erteilt werden darf, besonders aufmerksam den Zeitpunkt aber auch die Form der Auskunftserteilung zu beachten, wenn sie von den Medien zu bestimmten Personen befragt werden.

Im Zusammenhang mit einer disziplinarrechtlichen vorläufigen Dienstenthebung eines Beamten hat sich dieser zu Recht darüber beklagt, dass Medienvertreter vor der

Aushändigung des Bescheides an ihn ein Exemplar dieses Bescheides erhalten hatten.

Einer aus meiner Sicht zweifelsfreien Zeugenaussage zufolge wurde der Versuch unternommen, den Zeugen zu der vorläufigen Dienstenthebung an Hand des Bescheides, den dieser in den Händen eines Medienvertreters erkannt hatte, zu befragen.

Hier ist daran zu erinnern, dass eine Bestimmung des Strafgesetzbuches (§ 353 d Nr. 3) solche Verfahrensweisen unter Strafe stellt. Ein amtliches Schriftstück aus einem Disziplinarverfahren darf danach ebenso wenig wie die Anklageschrift oder andere Schriftstücke aus einem Straf- oder Bußgeldverfahren – auch nicht in wesentlichen Teilen – im Wortlaut öffentlich mitgeteilt werden, bevor eine öffentliche Verhandlung stattgefunden hat oder das Verfahren abgeschlossen wurde. Damit soll ein Entscheidungsdruck in eine bestimmte Richtung, im Sinne einer Vorverurteilung durch die Öffentlichkeit, verhindert werden.

Insbesondere Presseerklärungen der Staatsanwaltschaft sind daher mit großer Sorgfalt zu formulieren, damit das Recht auf informationelle Selbstbestimmung, z.B. in der Ausprägung des Steuergeheimnis, nicht verletzt wird (vgl. VG Saarlouis, NJW 2003, 3431).

14 Sonstiges

14.1 Akteneinsicht in Umweltschutzvorgänge

Das Umweltinformationsgesetz (UIG) gewährt jedem Bürger ein Recht auf freien Zugang zu den bei einer Behörde vorhandenen Informationen über die Umwelt.
Dadurch erhalten die Bürger die Möglichkeit, die Verwaltung bei der Anwendung der Umweltschutzvorschriften zu kontrollieren.
Nur wenn bestimmte Ausschlussgründe zum Schutz öffentlicher oder privater Belange vorliegen, ist der Informationsanspruch ausgeschlossen.
Die Prüfung, ob die Voraussetzungen für einen Ausschluss des Informationsanspruches vorliegen, ist naturgemäß nicht immer einfach; im Berichtszeitraum haben mehrfach Behörden bei mir angefragt, ob entsprechenden Anträgen auf Auskunft oder Akteneinsicht stattgegeben werden darf.

Meist war es allerdings so, dass eine Zuständigkeit meiner Dienststelle für die Beantwortung der Anfragen nicht gegeben war. In einem Fall etwa begehrte eine Naturschutzorganisation Einsicht in die Baugenehmigungsakte einer GmbH & Co. KG; in einem anderen Fall war über den Antrag auf Informationen über Betreiber von Anlagen nach der Störfallverordnung zu entscheiden. Wenn bei Gewährung des Auskunfts- oder Akteneinsichtsrechts Informationen über juristische Personen des öffentlichen oder Privatrechts bekannt gegeben werden, ist meine Dienststelle nicht der richtige Ansprechpartner, um zu beurteilen, ob der Anspruch auf Zugang zu den Umweltinformationen besteht.
Denn es ist Aufgabe des Datenschutzgesetzes und damit meiner Dienststelle, den Einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (§ 1 Saarländisches Datenschutzgesetz – SDSG). Eine Zuständigkeit meiner Dienststelle ist nur dann gegeben, wenn es um die Verarbeitung personenbezogener Daten – das sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person – geht.

Anders stellt sich die Situation in den Bundesländern dar, die Informationsfreiheitsgesetze erlassen haben und in denen die oder der Landesbeauftragte für den Datenschutz die Aufgabe einer/s Informationszugangsbeauftragten wahrnimmt.

In einem Fall, der an mich herangetragen wurde, war allerdings meine Zuständigkeit gegeben; in diesem Fall habe ich Bedenken gegen den Antrag auf Akteneinsicht geltend gemacht.

Eine Naturschutzorganisation verlangte Einsicht in die „Planungs- und Ausschreibungsunterlagen“ im Zusammenhang mit der Offenlegung eines Baches. Keine Bedenken habe ich gegen die Überlassung einer Kopie der Ausschreibung der Gemeinde geltend gemacht. Ich war allerdings der Auffassung, dass es nicht zulässig wäre, der Naturschutzorganisation die auf die Ausschreibung hin eingegangenen Angebote der Unternehmen zur Verfügung zu stellen. Es handelt sich hier um Geschäftsgeheimnisse, die gemäß § 8 Abs. 1 Satz 2 UIG nicht unbefugt zugänglich gemacht werden dürfen. Die Voraussetzungen für eine befugte Zugänglichmachung der Angebote der Unternehmen lagen meines Erachtens nicht vor. Denn es existiert keine Rechtsvorschrift, die dies ausdrücklich zulassen würde, im Gegenteil bestimmt die Verdingungsordnung für Bauleistungen ausdrücklich, dass die Angebote auf eine Ausschreibung und ihre Anlagen sorgfältig zu verwahren und geheimzuhalten sind. Auch eine Abwägung der Interessen des Antragstellers und der Allgemeinheit mit dem Interesse an der Wahrung der Geschäftsgeheimnisse stützt dieses Ergebnis. Denn, wie sich aus dem Antrag ergab, zielte das Interesse der Naturschutzorganisation nicht auf die Kenntnis der Angebotspreise sondern auf die Planungen der Gemeinde unter Naturschutzgesichtspunkten.

14.2 Datenschutz im parlamentarischen Bereich

Ein sehr schwerer Fall von Kindesmissbrauch im Saarland hat die Bevölkerung über die saarländischen Grenzen hinweg erschüttert.

Auch meine Dienststelle wurde über eine Eingabe mit der Angelegenheit befasst, als aus dem Protokoll einer nichtöffentlichen Ausschusssitzung des Landtages, in einem

überregionalen Presseorgan wortwörtlich zitiert wurde. Ein Verfahrensbeteiligter im Strafverfahren hat sich dadurch in seinen Rechten massivst verletzt gesehen.

An der Ausschusssitzung hatte auch ein Vertreter der Landesregierung teilgenommen, der über die Begleitumstände des Strafverfahrens im Ausschuss zu berichten hatte.

Ungeachtet meiner fehlenden Kontrollkompetenz für den Landtag, soweit er nicht Verwaltungsaufgaben wahrnimmt, musste festgestellt werden, dass der Kreis der in der Verwaltung tätigen Personen, die das Protokoll dienstlich zur Kenntnis nehmen durften, zwar überschaubar war, aber keinen Schluss auf die Ursächlichkeit datenschutzrechtlicher Verstöße gerade dieses Personenkreises zuließ. Das gleiche galt für den in den Ministerien tätigen Personenkreis.

Presseberichten zufolge haben sich die beiden damals im Landtag vertretenen Fraktionen gegenseitig beschuldigt, zur Identifizierung von Verfahrensbeteiligten durch die Medien beigetragen zu haben.

Ich möchte diesen Fall zum Anlass nehmen, zum wiederholten Mal auf die Notwendigkeit einer Datenschutzordnung für das Parlament hinzuweisen (vgl. 18. TB, TZ 18.10; 16. TB, TZ 6.4). Auch der Gesetzgeber ist an die Wahrung des Verfassungsrechts gebunden. Schon im eigenen Interesse und zu seiner Entlastung sollte er sich auferlegen, solche Vorfälle innerhalb des Parlaments restlos aufzuklären. Die Datenschutzordnungen für Parlamente in anderen Bundesländern sehen anstelle des hier von Verfassungs wegen nicht zuständigen Landesbeauftragten für Datenschutz ein innerparlamentarisches Datenschutzgremium für eine solche Datenschutzkontrolle vor.

Es wäre sehr zu begrüßen, wenn dieses Vorhaben auch im Saarland endlich in die Tat umgesetzt würde.

14.3 Fingerabdruck (Zeiterfassung; Verhinderung von Leistungsmissbrauch durch Asylbewerber)

In der Staatskanzlei gab es Überlegungen zu verschiedenen Einsatzmöglichkeiten neu entwickelter Fingerabdruckverfahren. Konkret ging es um die Abnahme von Fingerabdrücken von Asylbewerbern zur Verhinderung von Sozialleistungsmissbrauch sowie zum Zwecke der Zeiterfassung bei Behördenmitarbeitern.
Im Grundsatz gilt, dass der Fingerabdruck eines Menschen ein personenbezogenes Merkmal ist, dessen Erhebung einer Rechtsgrundlage bedarf. Wegen der Besonderheiten, die biometrische Daten im Gegensatz zu anderen personenbezogenen Daten aufweisen (historischer Ursprung als Erkennungsmittel von Kriminellen; hohes Zweckentfremdungsrisiko; Eignung als einheitliches Personenkennzeichen) halte ich die generalklauselartigen Vorschriften in den allgemeinen Datenschutzgesetzen als Legitimationsgrundlage für die Verarbeitung biometrischer Daten nicht für ausreichend. Ich halte es vielmehr für erforderlich, den Einsatz solcher Verfahren in speziellen, bereichsspezifischen Rechtsgrundlagen zu regeln. Bisher praktizierte Verfahren haben daher jeweils eine ausdrückliche gesetzliche Grundlage:
§ 81 b StPO (Fingerabdrücke für Zwecke der Durchführung eines Strafverfahrens).
§§ 41, 48 Ausländergesetz (Abnahme von Fingerabdrücken bei Ausländern bei Zweifeln über die Person oder die Staatsangehörigkeit des Betroffenen).
§ 16 AsylVerfG (Abnahme von Abdrucken aller 10 Finger eines Asylbewerbers zur Identitätsfeststellung).
§ 1 Abs. 4, 5 PersonalausweisG (Fingerabdruck im Personalausweis).

Die angedachte Abnahme von Fingerabdrücken bei Asylbewerbern zum Zwecke der Verhinderung von Sozialleistungsmissbrauch halte ich unter Zugrundelegung der Vorschrift des § 16 Asylverfahrensgesetz für unzulässig. Denn nach dieser Vorschrift ist die Verarbeitung und Nutzung von Fingerabdrücken nur zulässig für die Durchführung des Asylverfahrens, zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr. Die Unterlagen dürfen ferner für die Identifizierung unbekannter oder vermisster Personen verwendet werden.

Die Verhinderung von Sozialleistungsmissbrauch ist nach der gegenwärtigen Rechtslage kein zulässiger Nutzungszweck der gespeicherten Fingerabdrücke. Mangels einer entsprechenden Rechtsgrundlage wäre die Abnahme von Fingerabdrücken zu diesem Zweck daher unzulässig.

Wegen der Besonderheiten biometrischer Daten kann eine Verpflichtung der Beschäftigten zur Abgabe von Fingerabdrücken (hier zum Zwecke der Zeiterfassung) nicht auf die Vorschrift des § 31 Saarländisches Datenschutzgesetz gestützt werden, in dem die Datenverarbeitung in mehr allgemeiner Form bei Dienst- und Arbeitsverhältnissen geregelt ist. Standort einer entsprechenden Regelung könnte ein seit Jahren von den Datenschutzbeauftragten angemahntes Arbeitnehmerdatenschutzgesetz sein.
Ob allerdings der Zweck „Zeiterfassung“ die Abnahme von Fingerabdrücken rechtfertigen kann, erscheint mehr als zweifelhaft. Nach dem Grundsatz der Datenvermeidung und Datensparsamkeit, der auch in § 4 Abs. 4 Saarländisches Datenschutzgesetz seinen Niederschlag gefunden hat, ist bei der Auswahl zwischen verschiedenen Datenverarbeitungssystemen dem System der Vorzug zu geben, bei dem weniger Daten verarbeitet werden. Die bisherigen Zeiterfassungssysteme funktionieren ohne Fingerabdrücke, weshalb diesen Systemen nach dem genannten Grundsatz der Datenvermeidung und Datensparsamkeit der Vorzug zu geben ist.
Im Übrigen ergibt eine Verhältnismäßigkeitsprüfung, dass die geringfügigen Vorteile, die ein Fingerabdrucksystem zur Zeiterfassung eventuell mit sich bringt, außer Verhältnis zu dem in der Abnahme von Fingerabdrücken liegenden Eingriff und dessen Folgerisiken stehen.
Große Bedenken habe ich, die Datenverarbeitung in Arbeitsverhältnissen auf die Einwilligung der Bediensteten zu stützen. Eine echte Freiwilligkeit ist oft nicht gewährleistet, weil nicht auszuschließen ist, dass Beschäftigte ihre Einwilligung nur erteilen, um berufliche Nachteile zu vermeiden. Die Ungeeignetheit der Einwilligung ergibt sich auch aus dem Umstand, dass es keinen Sinn macht, ein System einzuführen, das bei der stets widerruflich zu haltenden Einwilligung oder Nichterteilung durch einen neuen Mitarbeiter nicht mehr eingesetzt werden kann.

Ich habe nach meiner Stellungnahme gegenüber der Staatskanzlei nichts mehr von der Angelegenheit gehört, so dass ich davon ausgehe, dass entsprechende Pläne derzeit nicht weiter verfolgt werden.

14.4 Flugdatenübermittlung in die USA

Trotz heftiger Proteste zahlreicher Bürgerrechts- und Datenschutzorganisationen, Politiker der EU und ihrer Staaten sowie der Datenschutzbeauftragten des Bundes und der Länder wurde den Flugpassagieren in die USA eine im Umfang keineswegs angemessene Übermittlung ihrer Daten an die amerikanischen Sicherheitsbehörden auferlegt.

Hintergrund dieses Verlangens der USA war das erhöhte Sicherheitsbedürfnis nach den Ereignissen des 11. September 2001.

Wegen der damit verbundenen mangelnden Beachtung der EG-Datenschutzrichtlinie hat der zuständige niederländische EU-Kommissar von Datenschutzorganisationen der Niederlande den „Big Brother Award“ erhalten. Diese Negativ-Auszeichnung wird neben weiteren Staaten auch in Deutschland an Firmen, Organisationen und Personen verliehen, die in besonderer Weise und nachhaltig die Privatsphäre von Menschen beeinträchtigen oder persönliche Daten Dritter zugänglich machen.

In einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder ist bereits im Vorfeld der – auch innerhalb der EU-Gremien – umstrittenen Entscheidung auf den zu großen Umfang der Daten, die geplante Zweckdurchbrechung bei der weiteren Datenübermittlung innerhalb der USA und insbesondere die fehlende Information der Flugpassagiere hingewiesen worden (Anlage 15.15).

Um das Verfahren transparent zu gestalten, hat die Gruppe der EU-Datenschutzbeauftragten nach Art. 29 der EG-Datenschutzrichtlinie unter Vorsitz des Bundesbeauftragten für den Datenschutz einheitliche Informationstexte für Passagiere, die in die USA fliegen, erstellt. Diese sind als Kurztext bei der Buchung einer Reise erhältlich oder im Internet unter

„http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm“

14.5 Geburtstagsdatum im Wählerinnenverzeichnis für die Wahl der Frauenbeauftragten

Bei dem Fall, den ich im Folgenden schildern möchte, handelt es sich sicherlich um keinen gravierenden Datenschutzverstoß, er ist aber ein Beispiel für eine gewisse Gedankenlosigkeit, die sehr oft Ursache für die Verletzung des Datenschutzes ist.

In einer Schule stand die Wahl zur Frauenbeauftragten an. Der mit der Durchführung der Wahl beauftragte Wahlvorstand erstellte das so genannte Wählerinnenverzeichnis, in das alle wahlberechtigten weiblichen Bediensteten der Schule aufzunehmen sind, und veranlasste dessen Aushang am Schwarzen Brett.
Eine Lehrerin beschwerte sich bei meiner Dienststelle, als sie feststellte, dass auch ihr Geburtsdatum vermerkt war. Diese Lehrerin hatte Recht mit ihrer Beschwerde, denn gemäß den Empfehlungen des damaligen Ministeriums für Frauen, Arbeit, Gesundheit und Soziales für die Wahl der Frauenbeauftragten in der Landesverwaltung sind in das Wählerinnenverzeichnis lediglich Familienname und Vorname der weiblichen Beschäftigten der jeweiligen Dienststelle aufzunehmen. Diese Regelung trägt dem datenschutzrechtlichen Grundsatz Rechnung, wonach personenbezogene Daten nur dann bekannt gegeben werden dürfen, wenn dies zur Aufgabenerfüllung erforderlich ist. Da das Geburtsdatum im vorliegenden Zusammenhang keine Rolle spielt, ist seine Bekanntgabe datenschutzrechtlich unzulässig.

Der Wahlvorstand hat prompt reagiert und die Geburtsdaten aus dem Wählerinnenverzeichnis entfernt.

14.6 Müllverwiegung

Seit Jahren wird öffentlich diskutiert, die Gebührenberechnung für die Abfallentsorgung auf eine andere Grundlage zu stellen. Gefordert wurde, die Gebühren nicht

mehr nach der Anzahl der Leerungen der Müllgefäße, sondern nach dem Abfallgewicht zu berechnen. Müllfahrzeuge und Abfallgefäße wurden in der Landeshauptstadt bereits auf diese Technik umgerüstet. Die Verbandsversammlung hat sich allerdings gegen eine Systemumstellung ausgesprochen und es in der Gebührensatzung bei dem bisherigen Berechnungsmodus belassen.

Einem Bürger, der bei dem zuständigen Entsorgungszweckverband eine Reduzierung der Abfuhrtermine wünschte, wurde entgegengehalten, bei dem in den letzten Monaten von seinem Haushalt produzierten Abfallgewicht könne seinem Antrag nicht stattgegeben werden. Der Betroffene wandte sich empört mit der Frage an meine Dienststelle, wie die Stadt dazu komme, seine Mülltonne bei der Abfuhr zu wiegen und das Abfallgewicht in einer Datei zu registrieren. Der Zweckverband hielt die Registrierung auf meine Anfrage hin für rechtmäßig. Die erfassten Daten würden sich nicht auf den Haushalt und die darin lebenden Personen beziehen, sondern in Bezug zu dem jeweiligen Anwesen stehen. Eine Auswertung der Daten sei generell und insbesondere auf das einzelne Anwesen bezogen derzeit nicht vorgesehen. Ich musste klarstellen, dass es sich um personenbezogene Daten der jeweiligen Gebührenschuldner handelt. Solange das Abfallgewicht nicht aufgrund satzungsrechtlicher Bestimmungen der Gebührenberechnung zugrunde zu legen ist, dürfen diese Angaben nicht in personenbeziehbarer Weise erfasst und weiterverarbeitet werden. Schließlich hat sich der Zweckverband nach Einschaltung des behördlichen Datenschutzbeauftragten der Stadt bereit erklärt, die Erfassungssoftware so ändern zu lassen, dass nur noch eine straßenbezogene Auswertung des Abfallgewichts möglich ist. Diese nicht mehr personenbeziehbare Auswertung ist aus nachvollziehbaren Gründen für die Tourenplanung der Abfallentsorgung notwendig.

14.7 Neues Denkmalrecht

Das saarländische Denkmalrecht wurde neu geordnet. Im Rahmen der Anhörung zu dem Gesetzentwurf habe ich vorgeschlagen, die Rechte der Betroffenen bei der Eintragung in die Denkmalliste zu verbessern. Im Gesetz wurde die Regelung aufgenommen, dass die Eigentümerinnen und Eigentümer vor der Eintragung anzuhören und von der Eintragung sowie deren Löschung zu unterrichten sind. Anhörung und

Unterrichtung dürfen nur unterbleiben, wenn ihre Durchführung unzumutbar ist, insbesondere wenn die betroffene Person nur mit unverhältnismäßig hohem Aufwand festgestellt werden kann.

14.8 Reform des Personenstandsrechts

Das seit 1957 nicht mehr grundlegend überarbeitete Personenstandsgesetz enthält aus der Sicht des Datenschutzes erhebliche Lücken:

- Der Zugang der wissenschaftlichen Forschung, auch von Familienforschern, zu den Personenstandsbüchern ist nicht geregelt. Genealogen machen den Datenschutz verantwortlich, dass sie nicht mehr – wie zu früherer Zeit – ohne Weiteres die Unterlagen bereits lange Verstorbener einsehen können. Das Personenstandsgesetz erlaubt jedoch nur den Betroffenen und ihren direkten Abkömmlingen Einsicht in die Bücher (§ 61 PStG). Andere Personen müssen ein rechtliches Interesse glaubhaft machen.
- Das Personenstandsgesetz geht davon aus, dass die Beurkundungen von Geburt, Eheschließung und Tod in „Büchern“ vorgenommen werden. Online geführte Personenstandsbücher haben keine rechtliche Grundlage.

Seit langer Zeit liegen Gesetzesentwürfe vor, die auch von den Datenschutzbeauftragten mitgetragen werden (vgl. meinen 16. TB 1996). Leider wurden diese Entwürfe nicht weiter verfolgt – vermutlich weil andere Vorhaben dringlicher erschienen. Im Berichtszeitraum ist ein neuer Vorentwurf eines Personenstandsrechtsreformgesetzes zur Diskussion gestellt worden, zu dem ich gegenüber dem Innenministerium Stellung genommen habe. Wie ich vor Redaktionsschluss erfahren habe, hat das Bundesinnenministerium auf der Basis dieses Entwurfs nunmehr das Gesetzgebungsverfahren für die Personenstandsrechtsreform eingeleitet.

14.9 Videoüberwachung

Im Saarland ist die Videoüberwachung durch öffentliche Stellen im allgemeinen Datenschutzrecht nicht gesetzlich geregelt. Nur die Polizei hat die Befugnis zur Video-

überwachung an so genannten Kriminalitätsschwerpunkten nach den im Saarländischen Polizeigesetz geregelten Voraussetzungen. Eine solche Videoüberwachung durch die Polizei wurde meines Wissens noch nicht durchgeführt. Daraus könnte man unter anderem schließen, dass die Sicherheitsbedürfnisse der saarländischen Bevölkerung selbst an Kriminalitätsschwerpunkten auch ohne diese Dauerüberwachung erfüllt werden konnten. Noch erfreulicher wäre der Schluss, es gäbe im Saarland keine derartigen Kriminalitätsschwerpunkte, die ein Vorgehen mittels Videoüberwachung rechtfertigten. Aus der Sicht des Datenschutzes wären beide Interpretationen zur tatsächlich fehlenden polizeilichen Videoüberwachung zu begrüßen.

Leider haben im Berichtszeitraum andere öffentliche Stellen einen Bedarf für die Videoüberwachung der in ihrer Verwaltung stehenden Gebäude und Grundstücke einschließlich der dort befindlichen Personen signalisiert. Mancher Bedarf lässt sich bei näherer Betrachtung auch durch weniger gravierende Maßnahmen als die Videoüberwachung befriedigen. So wäre einer Schule, die gegen Diebstahl, Vandalismus und Graffiti-Besprühungen mittels Videoüberwachung vorgehen wollte, auch durch eine einfache Umzäunung der Schule geholfen gewesen, die der Schulträger indes nicht finanzieren wollte. Die Videoüberwachung schien das weniger kostenträchtige Instrument zur Abwehr dieser Kriminalität zu sein, obwohl die Umzäunung dem Gebot der Datenvermeidung und Datensparsamkeit Rechnung getragen hätte.

Auch in anderen Bereichen (z.B. Justiz, Baubehörden) wurden Überlegungen angestellt, ob mit Videoüberwachungen eine Gebäudesicherung erzielt oder Baufortschritte festgehalten werden könnten. In beiden Fällen spielen dabei die Persönlichkeitsrechte der in den Gebäuden oder am Bau tätigen Personen aus der Sicht des Datenschutzes eine ausschlaggebende Rolle.

Als Dauerthema in einzelnen Kommunen kann man Planungen bezeichnen, Müllcontainer mittels Video beobachten zu lassen. Da auf Grund der stets schlanker werdenden Verwaltungen kommunales Personal kaum zur Verfügung steht, wird stets auch an den Einsatz privater Detektive zur Ermittlung von Müllsündern gedacht.

Hier stellt sich eine verfassungsrechtliche Vorfrage, die die datenschutzrechtliche Beurteilung insofern beeinflusst, als Tätigkeiten Privater im Kernbereich hoheitlicher

Aufgabenerledigung unzulässig sind. Die Ermittlung von Ordnungswidrigkeiten und Straftaten erfolgt ausschließlich im Gewaltmonopol des Staates, der diese Aufgabe nicht auf Private übertragen darf. Illegale Müllablagerungen stellen Ordnungswidrigkeiten und in Einzelfällen auch Straftaten dar, deren Verfolgung und Ahndung grundsätzlich den Angehörigen des öffentlichen Dienstes vorbehalten sind (Art. 33 Abs. 4 GG). Private dürfen lediglich bei technisch-mechanischen Hilfstätigkeiten ohne eigenen Entscheidungsspielraum tätig werden. Die beauftragten privaten Personen hätten es aber beispielsweise in der Hand, von einer Aufzeichnung oder Weitergabe der festgestellten Daten an die Ortspolizeibehörde in dem einen oder anderen Fall abzusehen. Der Ermessensspielraum bei der Datenverarbeitung in den hier zur Rede stehenden Phasen der Datenerhebung (Videobeobachtung) und Datenspeicherung (Videoaufzeichnung) ist daher einer so genannten datenschutzrechtlichen Auftragsdatenverarbeitung nicht zugänglich. Selbst wenn eine gesetzliche Grundlage vorhanden wäre, könnten Tätigkeiten Privater nicht in der vorgesehenen Art miteinbezogen werden.

Ich habe dementsprechend die Kommunen gebeten, von solchen Planungen Abstand zu nehmen.

Voraussetzung für die allgemeine Zulässigkeit der Videoüberwachung durch andere öffentliche Stellen als Polizeibehörden wäre zunächst die Schaffung einer Rechtsgrundlage, von der ich allerdings abraten möchte.

Für den privaten Bereich ist die Rechtsgrundlage in § 6 b Bundesdatenschutzgesetz vorhanden. Von dieser Möglichkeit wird reger Gebrauch gemacht, wie die alltäglichen Erfahrungen in Ladenpassagen, Kaufhäusern, Banken, Tankstellen. Bussen und Bahnen zeigen. Die Anzahl der bundesweiten Einsätze von Videokameras liegt inzwischen bei 400.000.

Aus meiner Sicht sollte der Staat sich beim Einsatz dieses Mittels – wegen der im privaten Bereich ohnehin stark fortschreitenden Technisierung – zurückhalten. Bürgerinnen und Bürger, aber auch die Bediensteten öffentlicher Stellen hatten bisher die Möglichkeit sich in öffentlich zugänglichen Bereichen überwiegend unbeobachtet zu bewegen. Im Saarland sind mir keine schwerwiegenden Sicherheitsdefizite be-

kannt geworden, die eine Videoüberwachung zusätzlich noch an diesen öffentlichen Stellen erforderlich erscheinen lassen. Zumindest kann mit weniger eingriffsintensiven Mitteln vielfach Abhilfe geschaffen werden.

Ich würde es außerordentlich bedauern, wenn auch dieses Stück der Freiheitskultur verloren ginge.

15 Anlagen

15.1 Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.
Sie sehen dabei folgende essentielle Punkte:

Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

- Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
- Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
- Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

Technischer Datenschutz

Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.
Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

Förderung von datenschutzgerechter Technik

Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus

für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung - für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur

Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung - als grundrechtssicherndes Verfahrenselement ergreifen muss.

Stärkung des Schutzes von Gesundheitsdaten

Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von

anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

Datenschutz und Gentechnik

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

Datenschutz im Steuerrecht

Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeach-

tet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und –speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.
Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

Arbeitnehmerdatenschutz

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.
Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

Stellung des Bundesdatenschutzbeauftragten

Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

Verbesserung der Informationsrechte

Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

15.2 Elektronische Signatur im Finanzbereich

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.1.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen„ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.
- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürge-

rinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.
Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.
- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.
Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,
- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,
- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,
- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,
- e-Government- und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,
- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,
- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

15.3 Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.
So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u.a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos

in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z.B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche

Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grds. selbst zu entscheiden,

- ob sie überhaupt verwendet wird,
- welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
- welche Daten zu löschen sind und wann das zu geschehen hat,
- ob sie im Einzelfall vorgelegt wird und
- welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin

- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach "der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

1. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht

dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

2. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

15.4 Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10 Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

15.5 TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz “Trusted Computing Platform Alliance” (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu

steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,
- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,
- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,
- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,
- der Zugang zum Internet und E-mail-Verkehr durch Softwarerestriktionen behindert würde,
- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,
- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und
- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und
- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

15.6 Transparenz bei der Telefonüberwachung

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, dass die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

15.7 Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der “Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)” entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstituti-

onen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. [1]

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. [2]

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und –Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

[1] Die Schutzprofile mit dem Titel “BISS – Benutzerbestimmbare Informationsflusskontrolle” haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

[2] Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

15.8 Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 2003

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz v. 28.3.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher - die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs — Personal Unblocking Keys —), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutz-schwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.3.2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines "vertragslosen" Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIMKarte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-

Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

15.9 Neuordnung der Rundfunkfinanzierung

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.
- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.
- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.
- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten — wie beispielsweise in der Nach-

barschaft oder bei privaten Adresshändlern — zu erheben, ausdrücklich erlaubt werden.

- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

15.10 Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. Juli 2003

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sogen. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr - wie vom geltenden Recht gefordert - in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,
- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nichtcodierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen

Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.
Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z.B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die
Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

15.11 Automatisches Software-Update

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. August 2003

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei - oftmals vom Nutzer unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne dass dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.
- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.
- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das - unbemerkte - Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die datenverarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss.

Personenbezogen Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

15.12 Gesundheitsmodernisierungsgesetz

Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.
- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z.B. mit data-warehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organi-

satorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass
- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.
Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

15.13 Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen” vorgelegt. Darin hat es festgestellt, dass
Die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2149; 2001; 3868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,
- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,
- in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,
- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,
- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,
- lediglich 24 % der Beschlüsse substanziell begründet werden,
- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,
- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören.

Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung - nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.
- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).
- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.
- Der Umfang des - seit Einführung der Vorschrift regelmäßig erweiterten - Straftatenkataloges des § 100 a StPO muss reduziert werden.
- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.
- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekann-

ten Geprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.
- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs.2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.
- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.
- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

15.14 Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 21.11.2003

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz (TKG) beschlossen. Dieser Entwurf sieht jetzt zwar - entsprechend der Forderung der Datenschutzbeauftragten - die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind

die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

15.15 Übermittlung von Flugpassagierdaten an die US-Behörden

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 13.02.04

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z.B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservie-

rungsdatenbanken nicht für Sicherheitszwecke sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.
Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II – System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet:
(http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm)
Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-

Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

15.16 Personennummern

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z.B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

15.17 Automatische Kfz-Kennzeichenerfassung durch die Polizei

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.
Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und –teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.
Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

15.18 Radio-Frequency Identification

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 20. November 2003 (Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;
dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und
soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.
Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

15.19 Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten. Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

15.20 Einführung eines Forschungsgeheimnisses für medizinische Daten

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

15.21 Datensparsamkeit bei der Verwaltungsmodernisierung

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

15.22 Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz

technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

15.23 Gravierende Datenschutzmängel bei Hartz IV

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. "Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung

nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

15.24 Staatliche Kontenkontrolle muss auf den Prüfstand

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. November 2004

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.
Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.
Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch

„Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.
Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.
Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

Sachverzeichnis

Abkürzungsverzeichnis

AO	Abgabenordnung
Artikel 10 G	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
AsylVerfG	Asylverfahrensgesetz
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BfV	Bundesamt für Verfassungsschutz
BGBl	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
CAPPS	Computer Assisted Passenger Prescreening System
DNA	Desoxyribonukleinsäure-Analyse (Molekular genetische Untersuchung)
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
eGovernment	Elektronic Government
ELSTER	Elektronische Steuererklärung
eMail	Elektronisch versandte Post
EU	Europäische Union
GBV	Grundbuchverfügung
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung für die Obersten Landesbehörden
GMBl	Gemeinsames Ministerialblatt des Saarlandes
IMSI	International Mobile Subscriber Identity
INPOL	Verbunddatei der Polizei
IT	Informationstechnik
JVA	Justizvollzugsanstalt
LfD	Landesbeauftragter für Datenschutz
LSVS	Landessportverband Saar
LfV	Landesamt für Verfassungsschutz

MBKW	Ministerium für Kultur, Bildung und Wirtschaft
NJW	Neue Juristische Wochenschrift
OWiG	Ordnungswidrigkeitengesetz
PDA	Personal Digital Assistent
PIN	Persönliche Geheimnummer
PStG	Personenstandsgesetz
PUK	Personal unblocking keys
Reg TP	Regulierungsbehörde für Telekommunikation und Post
RFID	Radio frequency identifikation
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SMG	Saarländisches Mediengesetz
SMS	Short Message Service
SPolG	Saarländisches Polizeigesetz
SSL	Secure Socket Layer: durch Verschlüsselung gesichertes Übertragungsverfahren im Internet
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVollzG	Strafvollzugsgesetz
TB	Tätigkeitsbericht
TCPA	Trusted Computing Platform Alliance
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TZ	Textziffer
UIG	Umweltinformationsgesetz
USB	Universal serial bus
VG	Verwaltungsgericht