21. Tätigkeitsbericht
des

Landesbeauftragten
für Datenschutz und Informationsfreiheit

für die Jahre 2005 und 2006

dem Landtag und der Landesregierung
vorgelegt am 21.11.2007

(Landtagsdrucksache 13/1660)

Der Landesbeauftragte
für Datenschutz und Informationsfreiheit 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: poststelle@lfdi.saarland.de
Internet-Angebot unter www.lfdi.saarland.de

Saarbrücken im November 2007

Geleitwort

Kumulierende Imponderabilien führten dazu, dass ich meinen 21. Tätigkeitsbericht 2005/2006 nicht so zeitnah vorzulegen vermochte, wie ich es mir eigentlich vorgenommen hatte. Gleichwohl bin ich der Überzeugung, dass dieser Tätigkeitsbericht dadurch weder an Bedeutung noch an Aktualität verloren hat. Im Gegenteil. Durch den zusätzlichen Zeitablauf mag sich noch deutlicher zeigen, dass die eine oder andere gesetzliche Änderung im Berichtszeitraum zwar Einschränkungen des Grundrechts auf informationelle Selbstbestimmung bedingt hat, keineswegs aber die mit diesen Änderungen verbundenen Hoffnungen, insbesondere auf ein Mehr an Sicherheit, erfüllt hat.

Danken darf ich an dieser Stelle dem Landtag des Saarlandes und insbesondere seinem Präsidenten für die gezeigte Unterstützung und das dokumentierte Wohlwollen. Danken will ich aber auch den Abgeordneten aller Fraktionen des Saarländischen Landtages, die sich für den Datenschutz – und nunmehr auch für die Informationsfreiheit – interessiert und engagiert haben. Ebenso will ich meine Verbundenheit gegenüber allen öffentlichen Stellen im Saarland zum Ausdruck bringen, die mich bei der Implementierung des Datenschutzes unterstützt haben.

Ganz besonders will ich aber meinen Kolleginnen und Kollegen danken. Sie haben es mir durch ihr Wissen, ihr Engagement und ihre Effizienz ermöglicht, die Geschäfte des Landesbeauftragten für Datenschutz und – seit November 2006 – für Informationsfreiheit unseres Landes erfolgreich zu führen und diesen Bericht vorzulegen.
Zwar spreche ich in meinem Bericht und auch anderswo, der Übung der Landes- und des Bundesdatenschützers gemäß, durchgängig in der Ich-Form von den Tätigkeiten meiner Geschäftsstelle.
Es ist aber klar und offenkundig, dass diese Tätigkeiten im Wesentlichen von meinen Mitarbeitern und Mitarbeiterinnen ausgeführt werden und ich ohne die mir gezeigte Unterstützung nur einen Bruchteil meiner Obliegenheiten erfolgreich wahrnehmen könnte.

In diesem Zusammenhang muss ich im Übrigen feststellen, dass nachdem die Institution einer Geschäftsstelle des Landesbeauftragten für Datenschutz seit über einem Vierteljahrhundert existiert, sie sich während meiner Amtszeit zwar entscheidend verjüngt hat, sie aber trotz dieser Verjüngung gleichwohl nunmehr langsam aber sicher an ihre Leistungsgrenzen stoßen wird. Die Anzahl der zu betreuenden Gesetzes- und untergesetzlichen Vorhaben steigert sich Jahr für Jahr. Auch die Anzahl der bei mir angebrachten Eingaben hat sich in meiner Amtszeit quasi verdoppelt. Darüber hinaus wurde mir im November 2006 die Aufgabe des Landesbeauftragten für Informationsfreiheit übertragen, ohne dass per heute die Mittel und Möglichkeiten meiner Geschäftsstelle hätten verstärkt werden können.

Roland Lorenz
Landesbeauftragter für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1 Vorbemerkung

An dieser Stelle wird vom berichtenden Datenschutzbeauftragten regelmäßig eine Art philosophisch – historisch – verfassungsrechtliche Grundsatzerklärung abgegeben. So habe ich es denn auch bislang gehalten.

Nachdem ich jedoch in der Vergangenheit feststellen musste, dass es im Eifer der Debatte immer wieder die zwei gleichen plakathaften (Schein)Argumente sind, die mir zur Erschütterung datenschutzfreundlicher Positionen vorgehalten werden und zwar: „Datenschutz wird zum Täterschutz“ und „Wer nichts zu verbergen hat, hat auch nichts zu befürchten“ will ich heute die Weiheräume des rechtswissenschaftlichen Doktorandenseminars mit seinen Verfassungsexegesen verlassen und meine datenschutzrechtlichen Bedenken in einer Zeit der Terrorismusbekämpfung und der Vorratsdatenspeicherung ebenfalls parabelhaft und apodiktisch vortragen.

Zum einen folgende Parabel oder richtiger, Geschichte aus dem Tierreich:
Ein Frosch, den man in einen Kessel kochendes Wasser wirft, springt sofort wieder hinaus. Der lebensrettende Sprung ist biologisch durch die Überlebensreflexe und Überlebenstriebe bedingt. Wenn man den gleichen Frosch in einen Kessel mit kaltem Wasser wirft und wird das Wasser erst allmählich erwärmt, so bleibt der Frosch im Kessel. Er unternimmt keinen Fluchtversuch. Zunächst mag ihm das langsame Wärmerwerden des Wassers nicht unangenehm sein. Später sind Überlebenswille und Überlebenskräfte erlahmt. Der Frosch geht elendiglich zu Grunde.[1])
Geht es uns auf dem Weg, wenn nicht in den Überwachungsstaat, so doch in die Überwachungsgesellschaft, vielleicht wie besagtem Frosch?

Und zum zweiten will ich die Bedenken, die meine Kolleginnen und Kollegen wie ich selbst aus Erfahrung gegen das Anlegen immer neuer Dateien geltend machen müssen, nicht mit einem geschichtlichen – teleologischen Exkurs zur Entwicklung der Zweckbindung bei LKW-Maut-Dateien oder Kontenevidenz – Dateien der Finanzverwaltung darlegen und begründen, sondern versuchen mit einem Zitat meines Lieb-

[1]Diese Geschichte aus dem Tierreich habe ich erstmals (zwar nicht bei Tiervater Brehm aber) in The Economist vom 29. September 2007, S. 62 als Zitat von Prof. Ross Anderson, Cambridge, gelesen. Sie wird auch von Peter Schaar in seinem Werk „Die verlorene Privatsphäre“, 2007, wiedergegeben.

lingsautoren Fjodor Dostojewski problembewußt zu machen. Und dies auf die Gefahr hin , dass das Zitat, aus dem Zusammenhang gerissen, als überzeichnend, unangemessen, gar böswillig gesehen wird. In seinen „Erinnerungen aus einem Totenhause“ stellt Dostojewski fest, die Agrargesellschaft des östlichen Sibiriens im mittleren Neunzehnten Jahrhundert unter besonderer Berücksichtigung der dorthin Deportierten betrachtend, dass “dort wo ein Trog ist, sich alsbald die Schweine sammeln“. Wie denn kürzer und prägnanter zum Ausdruck bringen, dass dort wo Schätze gehortet werden, sich alsbald Begehrlichkeiten artikulieren! Und das dort wo neue Datenansammlungen, sprich Datenschätze, aufgebaut werden, andere Datensammler alsbald ihr begründetes Interesse bekunden werden?

Nun, das Recht auf informationelle Selbstbestimmung ist eines der wichtigsten Bürgerrechte der Informationsgesellschaft. Es soll es auch bleiben. So werde ich denn weiterhin bei der Suche nach dem angemessenen Ausgleich zwischen der wirksamen Erfüllung staatlicher Aufgaben und der Wahrnehmung der Persönlichkeits- und Freiheitsrechte des Einzelnen weiterhin die Belange des Datenschutzes offensiv darstellen und implementieren.

2 Technisch-organisatorischer Datenschutz

2.1 eGo-Saar: Melderegister und Schattenspeicher

Im Rahmen der Novellierung des Saarl. Meldegesetzes wurde jedermann die Möglichkeit eröffnet, online eine Melderegisterauskunft zu erlangen.

Hierzu wurde die Möglichkeit geschaffen, dass öffentliche Stellen, die befugt sind, Daten aus dem Melderegister zu erhalten, die erforderlichen Daten elektronisch abrufen zu können. Darüber hinaus wurde jedermann die Möglichkeit eröffnet, ohne Angaben von Gründen eine Melderegisterauskunft auf elektronischem Wege zu bekommen.

Angesichts der heterogenen technischen Ausstattung der Kommunen wurde eine zentrale Stelle geschaffen, die diese Aufgabe übernimmt. An dieser zentralen Stelle im Rechenzentrum der Zentralen Datenverarbeitung Saar (ZDV Saar) wird ein tagesaktueller Datenbestand vorgehalten, der auf täglichen Zulieferungen aller Meldebehörden des Landes basiert. Dieser Datenbestand enthält alle bei den Meldebehörden gespeicherten Daten und steht für einen Abruf rund um die Uhr zur Verfügung.

Aus datenschutzrechtlicher Sicht war bei der technischen und organisatorischen Realisierung darauf zu achten, dass das bisherige Datenschutzniveau der Meldedaten weiterhin aufrecht gehalten wird. Entscheidend hierbei ist, dass trotz einem zentralen Vorhalten der Meldedaten, die vom Saarl. Meldegesetz vorgeschriebenen Zuständigkeiten der einzelnen Meldebehörden erhalten bleiben und technisch abgebildet werden. Die Speicherung und Weitergabe der Meldedaten ist nur als Datenverarbeitung im Auftrag möglich und wurde auch als solche vertraglich geregelt. Eine Vermischung der einzelnen Melderegister zu einem Landesmelderegister durfte es nicht geben und wurde durch eine logisch getrennte Speicherung der Daten sichergestellt. Die erforderliche tägliche Datenübertragung der Meldebehörden an den zentralen Schattenspeicher wird technisch unter Nutzung der sicheren VPN-Technologie in Verbindung mit einem Rechte- und Rollenkonzept realisiert. Somit wurden auch in

diesem Bereich die datenschutzrechtlichen Anforderungen nach Integrität und Vertraulichkeit der Daten beachtet und sichergestellt.

2.2 Ratsinformationssysteme

Bei vielen Kreis- und Gemeindeverwaltungen wird die Vor- und Nachbereitung der Gemeinderats- oder Kreistagssitzungen zunehmend durch Sitzungsmanagement-Systeme unterstützt. Dazu gehören z. B. die Vorlagenerfassung und –verwaltung, die Sitzungsplanung, die Erstellung der Tagesordnung, die Einladungen der Ratsmitglieder und sonstigen Teilnehmer, die Erstellung, Verwaltung, Archivierung der Niederschriften, die Beschlussausfertigung und –überwachung sowie die Sitzungsgeldverwaltung mit Anbindung an die einzelnen Kassenverfahren. Hinzu kommt immer mehr der Wunsch nach Anbindung der Systeme an das Internet zur Information und Interaktion mit dem Bürger, jedoch vor allem auch der Wunsch der Ratsmitglieder, Unterlagen von der Verwaltung auch elektronisch zu erhalten sowie auf die Info-Systeme der Verwaltung vom eigenen PC aus zugreifen zu können.

Solche Systeme mit verwaltungsinternem Sitzungsmanagement sind sehr verbreitet. Mit der entsprechenden Vergabe von Nutzungsrechten soll dafür gesorgt werden, dass nur berechtigte Teilnehmer das System im Rahmen der ihnen zustehenden Befugnisse nutzen, sprich die darin enthaltenen Daten bearbeiten bzw. zur Kenntnis nehmen können.

Datenschutzrechtlich problematisch wird es, wenn diese Verwaltungsinformationen auch extern, z.B. im Internet bereitgestellt werden sollen. Denn sowohl bei Einladungen zu Sitzungen als auch bei eventueller Veröffentlichung von Niederschriften öffentlicher Sitzungen muss darauf geachtet werden, dass dem Datenschutz Rechnung getragen wird. Insofern dürfen keine personenbezogenen oder –beziehbaren Daten im Internet abrufbar sein. Dies betrifft Tagesordnungspunkte aber auch eventuelle wörtliche Redebeiträge von Mandatsträgern oder sonstigen Sitzungsteilnehmern. Bei der Interaktion mit dem Bürger im Rahmen von eGovernment-Lösungen ist darauf zu achten, dass die Datenübertragung gesichert erfolgt und ansonsten die

Bürger über die damit verbundenen Risiken und gleichzeitig mögliche sichere Alternativen informiert werden.

Ein weiterer Problembereich stellt die Bereitstellung und Zustellung der Sitzungseinladungen, -unterlagen und -protokolle auf elektronischem Wege an die Ratsmitglieder dar. Einerseits gab es im Saarland dafür bis dato keine ausreichende Rechtsgrundlage. Andererseits kommen dann Unterlagen und in der Regel auch personenbezogene Daten in einen möglicherweise kritischen Bereich, in dem die Betroffenen den Datenschutzanforderungen oft nur unzureichend Rechnung tragen können.

Aus diesen Gründen habe ich anfragende Verwaltungen gebeten, bis zur Klärung der Rechtsgrundlage im Sinne der Normenklarheit auf entsprechende Lösungen zu verzichten. Diese Rechtsgrundlage wurde durch eine Änderung des KSVG im Rahmen des Gesetzgebungsverfahrens „Verwaltungsstrukturreformgesetz“ herbeigeführt, welche nun vom Saarländischen Landtag verabschiedet wurde und am 01.01.2008 in Kraft treten soll. Ich werde dazu beitragen, dass dann, wenn eine solche Weitergabe gesetzlich ermöglicht wird, die Verwaltung dafür Sorge trägt, dass eine elektronische Kommunikation mit Ratsmitgliedern in einem Rahmen eröffnet wird, der Gewähr für eine ausreichende Datensicherung und Datenschutz bietet.
In meinem Internet-Angebot ist ein entsprechendes „Merkblatt zur Behandlung personenbezogener Daten in Zusammenhang mit der Tätigkeit als Mitglied eines kommunalen Vertretungsorgans“ abrufbar.

2.3 Virtuelle Poststelle

Der kommunale Zweckverband eGo-Saar unternimmt große Anstrengungen den saarländischen Bürgerinnen und Bürgern, der Wirtschaft, aber auch den Verwaltungen untereinander Verwaltungsvorgänge zu modernisieren und vereinfachen und eine elektronische Kommunikation zu ermöglichen.

2006 erteilte der Zweckverband seinem Kompetenzteam „Virtuelle Poststelle“ den Auftrag bis Ende des Jahres technische und organisatorische Maßnahmen zu erarbeiten, um den zeitnahen Einsatz einer zentral betriebenen „virtuellen Poststelle“ zu

ermöglichen. Hierbei war zu berücksichtigen, dass die Kommunen im Saarland nicht in einem kommunalen Netz zusammengeschlossen sind und auch nicht über einen einheitlichen technischen Standard verfügen.
Bereits in der Konzeptionsphase wurde meine Dienststelle in die Überlegungen mit einbezogen und im Ergebnis meine datenschutzrechtlichen und technisch-organisatorischen Vorschläge bei der Umsetzung berücksichtigt.

Aufgrund der Überlegungen des Kompetenzteams wurde als Basistechnologie die Middleware „Governikus“ und als Endanwendung „Govello“ der Firma bremen online services (bos) für einen landesweiten Einsatz ausgewählt und in Betrieb genommen. Mit dem technischen Betrieb des Governikus, auf dem für jede Verwaltung ein Postfach eingerichtet ist, wurde das Informations- und Kommunikationsinstitut der Landeshauptstadt Saarbücken (IKS) beauftragt.

Mit Hilfe der in den Verwaltungen installierten Clients können Nachrichten OSCI-konform versandt und abgeholt werden. Somit ist es den Verwaltungen möglich, mit Hilfe einer sicheren und datenschutzgerechten Lösung Nachrichten auszutauschen.
Die Gewährleistung der aus Sicht des Datenschutzes wichtigen Aspekte Vertraulichkeit und Integrität der Daten wurde durch diese technische Lösung sichergestellt.

2.4 Internet-Angebot der Gemeinde Kleinblittersdorf als Muster

Nachdem auch die saarländischen Gemeinden und Kreise immer mehr dazu übergegangen waren, sich selbst und ihre Angebote im Interesse der Bürger auch im Internet zu präsentieren, hatte ich im Jahre 2001 die Anstrengung unternommen, alle damals verfügbaren Homepages aus datenschutzrechtlicher Sicht zu überprüfen und den zuständigen Bearbeitern Hinweise zur Überarbeitung zu geben.

Im Jahre 2003 kam die Gemeinde Kleinblittersdorf mit der Bitte auf mich zu, die nun anstehende Überarbeitung und Neukonzeption ihres Internet-Auftritts von Anfang an aus datenschutzrechtlicher Sicht zu begleiten. Es bot sich die Chance, dieses Ergebnis mustergültig auszubauen, so dass sich die anderen Gemeinden und Kreise daran orientieren konnten.

In einem längeren Prozess wurden das Konzept verfeinert, die Struktur festgelegt und die Inhalte aufbereitet. Neben einem korrekten Impressum, einer Datenschutzinfo und einem Haftungsausschluss wurde auch sichergestellt, dass den Aspekten einer Datenvermeidung und Datensparsamkeit des Datenschutzgesetzes Rechnung getragen wurde. So wurde möglichst die Nennung von Namen der Bediensteten vermieden und stattdessen z. B. funktionale Mail-Adressen verwandt. Bei allen Bildern des Angebots und Nennungen von Mandatsträgern mit ihren Funktionen wurde darauf geachtet, dass von den Betroffenen zur Veröffentlichung eine Zustimmung vorlag. Das entsprechende Formular war mit mir abgestimmt worden. Ein wichtiger Aspekt der Neugestaltung war auch die Barrierefreiheit des Angebots nach dem Behindertengleichstellungsgesetz, die es auch behinderten Mitbürgern erlauben sollte, die Texte, Grafiken und Bilder ohne größeren Aufwand und uneingeschränkt zur Kenntnis nehmen zu können. Im Mai 2005 konnte das Internet-Angebot der Gemeinde dann in einer öffentlichen Gemeinderatssitzung und unter Beteiligung der Presse zur allgemeinen Nutzung freigegeben werden.

2.5 Elektronisches Archiv mit Dokumentenmanagement bei der Zentralen Besoldungs- und Versorgungsstelle und der Zentralen Beihilfefestsetzungsstelle im Landesamt für Finanzen

Die saarländische Landesverwaltung nutzt für die Aufgaben der zentralen Besoldung und Beihilfefestsetzung Dialog- und Abrechnungsverfahren, die in Baden-Württemberg entwickelt und im Rahmen der Kieler Beschlüsse zur Verfügung gestellt worden waren. Zur Erleichterung des täglichen Arbeitsablaufs sollten nun alle Vorgangsdaten, insbesondere Stammblätter, Gehaltsmitteilungen, Kassenlisten und Beihilfebescheide sowie die Textverarbeitungs- und Mail-Daten unmittelbar in einer elektronischen Akte abgelegt werden. Damit sollten viele mechanischen Arbeiten wie Ablagetätigkeiten entfallen und auch Druckkosten eingespart werden. Einen entscheidenden Vorteil bot auch die schnellere, detailliertere und bessere Informationsbereitstellung durch ein elektronisches Dokumentenmanagementsystem. Der Einfachheit und Kostengünstigkeit halber sollte das System beim Zentrum für Informationsverarbeitung der Oberfinanzdirektion Stuttgart auf dem dort bereits vorhandenen Kernsystem als abgeschotteter Mandant mit Datenfernübertragung betrieben wer-

den. Der Transfer der Daten sollte verschlüsselt über das Testa-Behördennetz erfolgen.

In Abstimmung mit meiner Dienststelle wurde unter Berücksichtigung der Bestimmungen des § 11 SDSG eine Vorabkontrolle durchgeführt und ein Datenschutzkonzept erstellt. Die Auftragsdatenverarbeitung wurde unter Berücksichtigung der Anforderungen des § 5 SDSG datenschutzgerecht gestaltet. Der Auftragnehmer unterwarf sich meiner Kontrolle. Der Testbetrieb arbeitete ausschließlich mit anonymisierten Testdaten. Unter Berücksichtigung der besonderen Sensibilität wurde die Sicherheit der Datenübertragung auf den landesinternen Datenleitungen bis zur Testa-Kopfstelle durch eine Basis-Verschlüsselung sichergestellt. Das Löschungskonzept berücksichtigte auch die bei dieser Anwendung genutzte Speicherung auf optischen WORM-Platten. Insgesamt gelang es in begleitender Kooperation zwischen Fachbehörde und Datenschutz diesen ersten Einsatz eines elektronischen Archivs mit Dokumentenmanagementsystem in der saarländischen Landesverwaltung auch aus Sicht des Datenschutzes optimal auf den Weg zu bringen.

2.6 Penetrationstest des Landesdatennetzes

Auf meine Initiative hin vergab im Jahre 2005 die Zentrale Datenverarbeitung Saar (ZDV Saar) einen Auftrag an einen unabhängigen Auftragnehmer, um das Landesdatennetz einem Penetrationstest zu unterziehen. Der Vertragsabschluss und die daraus resultierenden Testläufe wurden ohne unsere Beteiligung im Vorfeld durchgeführt.

Nach Durchsicht des uns vorgelegten Vertrages stellten wir fest, dass datenschutzrechtliche Belange nur ansatzweise und sehr spärlich behandelt waren. Nach mehreren persönlichen Gesprächen sowohl mit der ZDV Saar als auch mit dem Auftragnehmer wurde uns die Beachtung der datenschutzrechtlichen Belange von beiden Seiten zugesagt. Im Verlauf des Testes und bei der Präsentation der Testergebnisse, bei denen wir nun einbezogen waren, konnten wir uns von der Erfüllung der Zusage überzeugen.

Zum Ergebnis des Penetrationstestes lässt sich Folgendes sagen: Es ergaben sich keine Schwachstellen schwerwiegenden Ausmaßes, die die Sicherheit des Landesdatennetzes durch Zugriffe von außen gefährden konnten. Lediglich ein Server, der sich allerdings außerhalb des geschlossenen Bereiches vor der Firewall befand, wies einige Schwachstellen auf, die in einer überalterten Konfiguration begründet waren. Bei genauerer Betrachtung stellte sich heraus, dass die Funktionalität dieses Servers anderweitig abgebildet werden kann. Der entsprechende Server konnte daher abgeschaltet werden.

Somit lässt sich letztendlich feststellen, dass es sich bei dem Landesdatennetz um ein geschlossenes, sicheres Netz handelt, in das – wenn überhaupt – nur mit sehr großem technischem Aufwand eingedrungen werden kann.

Allerdings stellte sich bei der Realisierung dieses Testes ebenso wie bei vielen anderen Projekten, die vertraglich geregelt werden, heraus, dass sehr oft das Festschreiben datenschutzrechtlicher Aspekte in den Vertragswerken sehr oft übersehen bzw. vergessen wird. Daher sollte bereits im Vorfeld, d.h. bei den ersten Planungen, der Landesbeauftragte für Datenschutz und Informationsfreiheit in die Beratungen und Überlegungen eingebunden werden.

2.7 IT-Dienstanweisungen des Ministeriums für Umwelt und des Ministeriums für Wirtschaft

Schon in der Vergangenheit hatte ich durch kooperative Erstellung von Muster-Dienstanweisungen dazu beitragen können, dass die Dienststellen der saarländischen Verwaltung ohne großen Aufwand in der Lage waren, auf Basis dieser Muster in eigenen Dienstanweisungen den Betrieb der Datenverarbeitung auch unter datenschutzrechtlichen Gesichtspunkten zu regeln.

Nach der Neufassung des Saarländischen Datenschutzgesetzes im Jahre 2002 bestand nun der Bedarf, diese Dienstanweisungen entsprechend zu aktualisieren, denn die Neufassung enthält unter anderem die Bestellung eines behördeninternen Datenschutzbeauftragten und die generelle Durchführung eine Vorabkontrolle vor der

Freigabe neuer oder wesentlich geänderter automatisierter Verfahren mit der Verarbeitung personenbezogener Daten.

Dankenswerterweise haben sich sofort die beiden Ministerien für Umwelt und Wirtschaft um eine Kooperation bei der Überarbeitung bemüht, wobei auch gleich die bisher getrennt geregelten Bereiche Faxbetrieb, Internet-Nutzung und Mail-Verkehr in die allgemeine Dienstanweisung integriert werden konnten. Diese konzeptionell unterschiedlich angelegten Dienstanweisungen konnten dann den anderen Ministerien und ihren nachgeordneten Dienststellen als Muster zur Verfügung gestellt werden, was diesen die Arbeit wesentlich erleichtert hat. Diese Muster stehen jetzt allen anderen Dienststellen der Landesverwaltung zur einfachen Umsetzung zur Verfügung.

2.8 IT-Sicherheitskonzept der HTW

2006 trat die HTW mit der Bitte an meine Dienststelle heran, sie bei der Erstellung einer Risikoanalyse und des daraus resultierenden IT-Sicherheitskonzeptes zu unterstützen.
Bei der Erstellung dieser Papiere wurde das IT-Grundschutzhandbuch des BSI zu Grunde gelegt. Nach vielen gemeinsamen Gesprächen in der Entstehungsphase dieser Papiere wurde von Seiten der HTW ein Konzept entwickelt, das allen Aspekten Rechnung trägt und in meinem Internetangebot allen Verwaltungen im Saarland als Musterdokument zum Abruf angeboten wird.

In diesem Fall zeigt sich, dass eine frühzeitige Einbindung meiner Dienststelle bei der Erstellung erforderlicher Unterlagen hilfreich sein und somit auch innerhalb eines kurzen Zeitraumes eine Dokumentation angefertigt werden kann, die den heutigen Anforderungen in vollem Umfange gerecht wird.

3 Justiz

3.1 Einführung biometrischer Ausweisdokumente

Mit der Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 wurden die Mitgliedsstaaten verpflichtet bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen. Seit dem 01. November 2005 wird auf Reisepässen in einem integrierten Chip, der sich im Passdeckel befindet, ein digitalisiertes Lichtbild gespeichert. Die Bundesrepublik Deutschland hat hier eine Vorreiterrolle übernommen und als erstes Land mit der Umsetzung der EG-Verordnung begonnen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder rügte diese übereilte Vorgehensweise in ihrer Entschließung vom 01. Juni 2005 zur Einführung biometrischer Ausweisdokumente, da das Verfahren technisch noch nicht hinreichend ausgereift war und demzufolge sowohl die technische Reife und der Datenschutz als auch die technische und organisatorische Sicherheit nicht gewährleitstet werden konnten (siehe Anlage 17.24).

Auch die 27. Internationale Konferenz der Datenschutzbeauftragten in Montreux vom 16. September 2005 hatte eine Resolution verabschiedet und wirksamere Schutzmaßnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, gefordert. Darin wurde auch auf die strikte Trennung zwischen biometrischen Daten beharrt, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z.B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden. Zuletzt wurden die technischen Beschränkungen auf den ausschließlichen Zweck der Identifizierung durch momentanen Datenabgleich postuliert (siehe Anlage).

Die EG-Verordnung sieht weiterhin die Einführung von Fingerabdrücken in den sogenannten ePass als zweites biometrisches Merkmal vor, deren Realisierung bis zum 28. Februar 2008 erfolgt sein soll. Die Bundesregierung hatte daher bereits am 05. Januar 2007 den Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften vorgelegt, in dem ein durchgängig elektronisches Verfahren der Passbeantragung angestrebt wurde. Der Deutsche Bundestag hat in seiner 100. Sitzung am 24. Mai 2007 aufgrund der Beschlussempfehlung und des Berichts des Innenausschusses den von der Bundesregierung eingebrachten Gesetzesentwurf an-

genommen und das Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften beschlossen. Die zur Identitätsprüfung erhobenen Daten dürfen nunmehr auch für einen automatisierten Abgleich mit erkennungsdienstlichen Dateien der Polizeivollzugsbehörden verwendet werden. Im Pass gespeicherte Daten, die die Polizeivollzugsbehörden zur Überprüfung der Echtheit des Passes oder der Inhaberidentität auslesen und verwenden dürfen, müssen nicht umgehend gelöscht werden, wenn die Daten im Rahmen eines Strafverfahrens oder zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung noch benötigt werden. Ferner wurden noch die Möglichkeiten des automatisierten Abrufs von im Passregister gespeicherten Daten durch die Polizeivollzugsbehörden erweitert. Als datenschutzrechtlich bedenklich sehe ich hier vor allem eine nunmehr für den Polizeivollzugsdienst bestehen Möglichkeit auf erkennungsdienstliche Daten wie Lichtbilder und Fingerabdrücke zugreifen zu können, welche bisher nach den Polizeigesetzen der Länder und der Strafprozessordnung nicht bestanden hat.

3.2 Eingabe wegen unbefugter Übersendung einer Anklageschrift

Nach § 406e Abs.1 StPO kann ein Rechtsanwalt die Akten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, einsehen sowie amtlich verwahrte Beweisstücke besichtigen, soweit er hierfür ein berechtigtes Interesse darlegt. Handelt es sich bei dem Verletzten um einen Nebenkläger nach § 395 StPO, so ist die Darlegung des berechtigten Interesses nicht erforderlich. Dem Verletzten, der ein berechtigtes Interesse darlegt, kann gemäß § 406e Abs.5 StPO der zuständige Staatsanwalt Auskünfte oder Abschriften aus den Akten erteilen.

Im konkreten Fall übersandte die Staatsanwaltschaft Ihre Anklageschrift an die rechtsanwaltliche Vertretung der Klägerin, obwohl diese bereits im Vorfeld erklärt hatte, dass ihrerseits kein Bedarf an Akteneinsicht besteht und diese daher auch nicht beantragt wird. Mithin lagen die Voraussetzungen des § 406e StPO nicht vor, so dass die Anklageschrift ohne Rechtsgrundlage an die Rechtsanwälte der Klägerin übersandt wurde. Ich habe daher die Staatsanwaltschaft um Stellungnahme zur Sach- und Rechtlage gebeten, woraufhin mir mitgeteilt wurde, dass seitens der Ge-

neralstaatsanwaltschaft ein Ermittlungsverfahren nach § 203 StGB, wegen Verletzung von Privatgeheimnissen, eingeleitet worden sei und hinsichtlich des vorgenannten Verfahrens eine neue staatsanwaltliche Bearbeitungszuständigkeit vergeben worden sei.

3.3 Vorratsdatenhaltung bei Telekommunikationsverbindungsdaten

Die Bundesregierung hatte seit längerem beabsichtigt, ein Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden zu schaffen. Hierzu wurden entsprechende rechtswissenschaftliche und rechtstatsächliche Gutachten eingeholt. Aufgrund dieser Dossiers wurde seitens der Bundesregierung insbesondere im Bereich der Telekommunikationsüberwachung ein Änderungsbedarf hinsichtlich technischer Neuerungen und Schwierigkeiten in der Strafverfolgungspraxis bei der Anwendung der bisherigen gesetzlichen Regelungen gesehen. Ein erster Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wurde daher im November 2006 vorgelegt. In diesem Entwurf wurde das Recht der strafprozessualen Ermittlungsmaßnahmen umfassend überarbeitet. Geplant ist die Einführung eines neuen § 101 in die StPO, der „für alle eingriffsintensiven verdeckten Ermittlungsmaßnahmen“ Verfahrensregelungen wie Kennzeichnungspflicht, Benachrichtigungspflicht, Definition des zu benachrichtigenden Personenkreises, Erfordernis einer gerichtlichen Zustimmung zur Zurückstellung der Benachrichtigung, Nachträglicher gerichtlicher Rechtschutz und Löschungspflicht enthält.
Im nunmehr vorliegenden Gesetzesentwurf vom 27. April 2007 wurde sodann aber der Schutz der Zeugnisverweigerungsberechtigten, insbesondere der Journalisten, verringert, Benachrichtigungspflichten gegenüber Betroffenen aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet. Weiterhin wurden die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt. Die Datenschutzbeauftragen des Bundes und der Länder haben in ihrer diesbezüglichen Entschließung im Juni 2007 deutlich zum Ausdruck ge-

bracht, dass dieser Gesetzesentwurf einen unverhältnismäßigen, massiven Eingriff in die Privatsphäre der Bürgerinnen und Bürger darstellt, die in ihren Grundrechten hierdurch in einem nicht tolerierbaren Maß eingeschränkt werden. Deshalb ist der Gesetzesentwurf in der bislang vorliegenden Fassung nach meiner Rechtsauffassung als verfassungswidrig zu beurteilen.

4 Polizei

4.1 Akkreditierungsverfahren zur Fußball-WM 2006

4.1.1 Testlauf zum Confederations-Cup

Als Test für das Akkreditierungsverfahren wurden bereits beim Confederations-Cup des Jahres 2005 einige Personen einer Zuverlässigkeitsüberprüfung unterzogen. Aufgrund einer Eingabe habe ich dieses Verfahren einer Prüfung unterzogen.

Die personenbezogenen Daten der Bewerber für eine Tätigkeit im Rahmen des Confederations-Cup wurden den Landeskriminalämtern vom Deutschen Fußballbund e.V. elektronisch zur Verfügung gestellt. Eine schriftliche Einwilligung der Bewerber lag vor. Die Daten wurden mit den Beständen des Landeskriminalamtes abgeglichen. Im Falle eines Treffers fand eine Einzelbewertung statt. Hierzu wurden die festgestellten Straftaten mit einem Kriterienkatalog abgeglichen, der von den Länderpolizeien gemeinsam erarbeitet worden war. Entsprach die Schwere der Straftat einer im Kriterienkatalog enthaltenen Konstellation wurde der Bewerber abgelehnt.

Das Verfahren wurde nicht beanstandet.

4.1.2 Fußballweltmeisterschaft 2006

Die Fußballweltmeisterschaft 2006 war nicht nur in sportlicher Hinsicht ein herausragendes Ereignis. Die Gewährleistung der Sicherheit bedeutete für die Organisatoren eine immense Herausforderung.

Alleine dass rund 150.000 Menschen bei dieser Großveranstaltung unterschiedliche Aufgaben wahrgenommen haben und sich deshalb einem Überprüfungsverfahren unterziehen mussten, lässt mich als Datenschutzbeauftragten zumindest „frösteln“. Die Rechtsgrundlage für die Übermittlung der personenbezogenen Daten an Polizei und Verfassungsschutz war die schriftliche Einwilligung der Betroffenen.

Aufgrund der Tatsache, dass das Saarland nicht über geeignete Sportstätten verfügt und deshalb nicht zu den ausrichtenden Bundesländern der Fußball-WM gehörte, war die Anzahl der überprüften Personen außerordentlich gering. Das Verfahren führte im Saarland zu keiner Ablehnung der überprüften Personen.

4.2 Prüfung der Datei „Gewalttäter Sport“

Die Erfassung in der Datei „Gewalttäter Sport“ führt zu weitreichenden Einschränkungen für die Betroffenen im unmittelbaren zeitlichen Zusammenhang von sportlichen Großereignissen, wie im letzten Jahr, der Fußball WM. Eingaben von Betroffenen haben gezeigt, dass durch unrechtmäßige oder veraltete Speicherungen verschärfte Kontrollen bei Auslandsreisen durchgeführt und sogar Auslandsreisen durch vorübergehende Einbehaltung der Personalpapiere verhindert worden sind.

Aus einer Übersicht des Bundeskriminalamtes vom September 2005 ging hervor, dass im Saarland überproportional viele Einträge (207) im Fahndungsbestand vorhanden waren. Im Vergleich dazu wiesen Bayern 407 und Rheinland Pfalz 149 Einträge auf. Vor diesem Hintergrund wurde die Datei „Gewalttäter Sport“ zu Beginn des Jahres 2006 einer stichprobenartigen Prüfung unterzogen.

Aus einer aktualisierten Liste mit 195 Einträgen wurden 13 Einträge nach dem Zufallsprinzip ausgewählt. Dabei wurden folgende Feststellungen getroffen:

- In 2 Fällen waren die Einträge bereits gelöscht. Fristablauf war noch nicht eingetreten. Die Löschung erfolgte, weil die betroffenen Personen nach den Feststellungen der szenekundigen Beamten nicht mehr in Erscheinung getreten waren. Die Löschungsbelege wurden vorgelegt.
- In 2 Fällen wurden Strafverfahren eingeleitet. Die entsprechenden Aktenzeichen waren im Vorgangsbearbeitungssystem DIPOL durch die Geschäftsstelle erfasst. Im Erfassungsbeleg waren die Aktenzeichen (noch) nicht vermerkt.
- In 3 Fällen waren als Aktenzeichen „ES“-Zeichen (ES = Ersuchen) angegeben. Es handelt sich dabei um Tagebuchnummern, über die die entsprechenden Vorgänge intern zugeordnet werden. Durch Ingewahrsamnahme der Personen wurde

eine sogenannte Drittort-Auseinandersetzung verhindert. Strafverfahren wurden nicht eingeleitet.

- In 5 Fällen enthielt das Feld Aktenzeichen den Eintrag „u“ (für unbekannt). Alle Personen waren nach Feststellungen der Polizei aggressiv gegen Fans der Gastmannschaft vorgegangen. Auseinandersetzungen wurden durch Schlagstock- und Diensthundeeinsatz verhindert. Zur Abwehr weiterer Straftaten wurden die Personen festgehalten und einer Personenkontrolle unterzogen. Strafverfahren wurden nicht eingeleitet.
- In einem Fall war im Feld Aktenzeichen kein Eintrag vorhanden. Obwohl die Person anlässlich tätlicher Auseinandersetzungen zwischen verfeindeten Fangruppen in Gewahrsam genommen wurde, ist ein Strafverfahren nicht eingeleitet worden.

Aus datenschutzrechtlicher Sicht wurden zu diesen Feststellungen folgende Forderungen aufgestellt:

- Personen, die länger nicht mehr auffällig waren, sind durch die szenekundigen Beamten zu löschen. Da es keinen erkennbaren Grund gibt irgendwelche Unterlagen über die Betroffenen vorzuhalten sind alle Unterlagen zu vernichten. Hierzu gehören auch die Löschungsbelege.
- Aktenzeichen der Staatsanwaltschaft müssen zeitnah Eingang in die Akten finden.
- In insgesamt 9 Fällen (von 13 geprüften) wurde kein Strafverfahren eingeleitet. Aus der Sachverhaltsschilderung geht hervor, dass beispielsweise §§ 125 ff StGB (Landfriedensbruch etc.) oder §113 StGB (Widerstand gegen Vollstreckungsbeamte) in Betracht zu ziehen waren und entsprechende Verfahren aus hiesiger Sicht bei genauerer Sachverhaltsschilderung durchaus mit Aussicht auf Erfolg hätten durchgeführt werden können. Der gesamte Datenbestand ist daraufhin zu überprüfen, ob weitere gleich gelagerte Fälle nach dem Legalitätsprinzip (§152 StPO) an die Staatsanwaltschaft weiterzuleiten sind.

4.3 Erlass zur Nutzung von Daten aus dem Personalausweis- und Passregister zum Zweck der Fahreridentifizierung

Das Ministerium für Inneres, Familie, Frauen und Sport hat mit Erlass vom 14.04.2005 -Az.: D4-B-1-1; Tbg-Nr. 15/05 – die Nutzung von Daten aus dem Personalausweis- und Passregister zum Zweck der Fahreridentifizierung neu geregelt. Im Gegensatz zu den vorhergehenden Erlassen aus den Jahren 1990, 1994 und 1999 ist dabei die zuvor bestehende Verhältnismäßigkeitsgrenze für den Verwarnungsgeldbereich, bei der eine Ermittlung anhand der Register unterbleiben sollte, gänzlich entfallen. Demnach kann nunmehr jede Ermittlungsbehörde zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr auch bei geringfügigen Verstößen im Verwarngeldbereich Daten aus dem Personalausweis- und Passregister im Rahmen eines Bildvergleichs erheben.

Derartige Verstöße im Verwarngeldbereich sind dem Bagatellunrecht im Straßenverkehr zuzurechnen, welches hier dem Recht auf informationelle Selbstbestimmung gegenübersteht, in das durch den Lichtbildvergleich, wenn auch auf gesetzlicher Grundlage, eingegriffen wird. Bei der Abgabe eines Lichtbildes zur Aufnahme in den Personalausweis handelt es sich um eine zwangsweise staatliche Vorgabe, da jedermann einen Personalausweis mit Lichtbild oder stattdessen einen Pass besitzen muss. Das Lichtbild wird bei Abgleich mit dem Fahrerfoto einer zweckändernden Datenverarbeitung zugeführt. Für die Heranziehung von Bildern bedarf es einer Abgrenzung zwischen den erheblichen Fällen, die unter Abwägung mit dem Recht auf informationelle Selbstbestimmung einen solchen Eingriff ermöglichen und den weniger erheblichen Fällen. Diese Abgrenzung ist vom Gesetz- und Verordnungsgeber bei der Festlegung der eintragsfähigen Verkehrsverstöße erfolgt und gewährleistet hierdurch eine klare Nachvollziehbarkeit für den Rechtsanwender sowie den Betroffenen.

Aus Sicht des Datenschutzes ist das mit Verfassungsrang aufgestellte Gebot der Verhältnismäßigkeit einzuhalten, was ich gegenüber dem Ministerium für Inneres, Familie, Frauen und Sport wiederholt und vehement vor Inkrafttreten des Erlasses gefordert habe.

Zu meinem Bedauern wurden diese datenschutzrechtlichen Grundsätze im Erlass vom 14.04.2005 nicht berücksichtigt. Es bleibt abzuwarten wie sich die Gerichte in eventuellen Verfahren positionieren werden.

4.4 Gesetz zur Erhöhung der öffentlichen Sicherheit im Saarland

Im November 2006 wurde meiner Dienststelle ein erster Entwurf eines Gesetzes zur Erhöhung der öffentlichen Sicherheit im Saarland im Rahmen des externen Anhörungsverfahrens mit der Bitte um Stellungnahme übersandt. Dieser sah neben mit Grundrechtseinschränkungen verbundenen, einschneidenden Änderungen im Saarländischen Polizeigesetz auch eine Anpassung des Saarländischen Datenschutzgesetzes vor.

Unsere Sicherheitsbehörden im Saarland leben vom Vertrauen der Bevölkerung und besitzen es auch. Gerade deshalb darf dieses Vertrauen nicht durch überzogene oder überflüssige Eingriffsbefugnisse untergraben werden.

Aus meiner Sicht stellte einerseits die beabsichtigte Einführung der präventivpolizeilichen Telekommunikationsüberwachung und andererseits die Möglichkeit der Videoüberwachung für alle öffentlichen Stellen im Rahmen der einfachen Aufgabenerfüllung, einen wesentlichen, neuerlichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Hinsichtlich der Telekommunikationsüberwachung konnte kein entsprechender Bedarf nachgewiesen werden. Was den Bereich der Videoüberwachung anbelangt, so hatte ich wiederholt - auch in vorangegangenen Tätigkeitsberichten - auf die Gefahr der „Jedermann-Überwachung“ hingewiesen, die mit Sicherheit einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte darstellt:

Die Aufgabenerfüllung öffentlicher Stellen mittels Videoüberwachung kann allenfalls dann als verhältnismäßig angesehen werden, sofern hochrangige Rechtsgüter konkret gefährdet sind.

Außerhalb des Berichtszeitraumes wurde mit der LT-Drs 13/1313 vom 16.04.2007 sodann eine vollständig überarbeitete Fassung des Gesetzesentwurfes vorgelegt, der meinen, aber auch den Anregungen und Forderungen anderer Angehörter teilweise Rechnung trug.

Das Gesetz zur Erhöhung der öffentlichen Sicherheit im Saarland ist außerhalb des Berichtzeitraumes am 12. September 2007 in zweiter Lesung vom Landtag des Saarlandes verabschiedet und kürzlich im Amtsblatt des Saarlandes vom 02.11.2007 veröffentlicht worden. Es soll am 01.01.2008 in Kraft treten.

Vor diesem Hintergrund will ich eine ausführliche Würdigung dieses Gesetzes im entsprechenden Bericht vornehmen. Ungeachtet dessen will ich gleichwohl zu diesem Gesetz vorab einige Anmerkungen machen:

Für den Bereich der Videoüberwachung verbleibt die Befugnis, Bildaufzeichnungen zur Gefahrenabwehr für die öffentliche Sicherheit vorzunehmen, grundsätzlich bei der Vollzugspolizei. Dies begrüße ich. Allerdings ist die in § 27 des SPolG festgeschriebene Sonderbefugnis der Ortspolizeibehörden zur Videoüberwachung im Rahmen der Erfüllung ihrer durch Rechtsvorschrift zugewiesenen Aufgaben, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist, (so z.B. zur Bekämpfung illegaler Müllablagerung) meines Erachtens weitgehend als unzulässige Vorratsdatenspeicherung anzusehen. Darüber hinaus handelt es sich hierbei nicht um eine Präventionsmaßnahme, sondern im Ergebnis vielmehr faktisch weitgehend um eine Maßnahme zur Verfolgung von Ordnungswidrigkeiten, welche der repressiven Polizeiarbeit zu zuordnen ist.
Im Übrigen vertrete ich die Auffassung, dass das Anfertigen von Bildaufzeichnungen zur Abwehr einer jeden Gefahr für die öffentliche Sicherheit nicht verhältnismäßig ist (z.B. auf Grund mangelnder Erforderlichkeit, Eignung oder wegen Verletzung des Übermaßverbots). Deshalb regte ich an, den Wortlaut der Begründung, dass es sich um „Rechtsverstöße von erheblichem Gewicht“ handeln muss, als Tatbestandsvoraussetzung im Gesetzestext zu verankern. Dies alleine ist geeignet, mit Sicherheit auszuschließen, dass die Videoüberwachung nicht schon auf Grund einer „Generalklausel“ zur beliebigen Gefahrenabwehr zulässig wird.

Weiterhin wurde die Möglichkeit der automatisierten Kfz-Kennzeichenerfassung im Saarland ausschließlich zu präventiven Zwecken eingeführt. Sie soll der Vollzugspolizei bei Kontrollen nur zur Abwehr einer Gefahr zustehen. Es ist beabsichtigt das bayerische automatisierte Kennzeichenlesesystem auch im Saarland zur Anwendung zu bringen. Im Rahmen des Parlamentarischen Anhörungsverfahrens habe ich die Unbestimmtheit und Weitläufigkeit des Begriffes „Fahndungsbestand“ moniert. Der Begriff ist bis dato nämlich weder Gegenstand einer gesetzlichen Definition noch einer Auslegung durch die Rechtsprechung gewesen. Es bleibt daher abzuwarten, welche Daten unter den Begriff „Fahndungsbestand“ gefasst werden.
Unter Umständen wird festzustellen sein, ob in diesen sogenannten „Fahndungsbestand“ Daten Eingang finden, deren Aufnahme in diesen Bestand die vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Grundsätze verletzen.
Anzumerken ist, dass die Verhältnismäßigkeit der Maßnahme höchst umstritten bleibt. Zudem besteht die Sorge, dass eine flächendeckende Überwachung aller Kfz-

Nutzer nur noch eine Frage der Ausgestaltung und geringfügiger Änderungen technischer Systeme darstellt.
Ich werde die tatsächliche Umsetzung aufmerksam verfolgen.

Mit § 28a SPolG wurde nach meinem Dafürhalten das Urteil des Bundesverfassungsgerichts zum Großen Lauschangriff jedenfalls hinsichtlich der Wohnraumüberwachung in vertretbarer Weise umgesetzt. Auch der nach § 53 StPO besonderes geschützte Personenkreis der Berufsgeheimnisträger wird nunmehr in Gänze angemessen geschützt. Aus meiner Sicht wäre hier lediglich noch eine nähere Bestimmung der Eingriffsvoraussetzungen wie beispielsweise in § 29 des rheinlandpfälzischen Polizeigesetzes wünschenswert gewesen.
Hinsichtlich der Telekommunikationsüberwachung hatte ich im Übrigen empfohlen, die Neuregelungen des Bundesgesetzgebers zu §§100 ff StPO abzuwarten. Erst nach dieser Neuregelung wird eine eventuelle Regelungslücke für präventiv polizeiliches Vorgehen überhaupt erkennbar werden.
Die Verankerung der von mir angeregten Berichtspflicht der Landesregierung gegenüber dem Landtag über die Anzahl durchgeführter Telekommunikationsmaßnahmen kann ich bereits jetzt positiv bewerten. Sie wirkt einer Bagatellisierung dieser Maßnahme entgegen.

Bemerken will ich, dass im parlamentarischen Abänderungsverfahren ohne erneute Anhörung des Landesbeauftragten für Datenschutz und Informationsfreiheit § 30 Abs.2 des SPolG sowie § 3 des SVerfSchG geändert worden sind.

Durch die Änderung des § 30 Abs.2 des SPolG ist der bisherige enge Begriff der „Straftat“ durch den weiter gefassten Begriff der „mit Strafe bedrohten Tat“ ersetzt worden. Damit hält die Speicherung der Daten von Kindern - unabhängig vom Alter - die als Intensivtäter ermittelt werden, Einzug in das Saarländische Polizeirecht.

Im Übrigen habe ich hinsichtlich der Frage einer gesetzlichen Verankerung der „Online-Durchsuchung im saarländischen Polizeirecht“ empfohlen, sowohl das weitere Gesetzgebungsverfahren auf Bundesebene als auch vor allem die anstehende Entscheidung des Bundesverfassungsgerichts abzuwarten.

Auch habe ich mich ohne Erfolg gegen die durch das Gesetz zur Erhöhung der öffentlichen Sicherheit im Saarland vorgesehene Einführung einer Rechtsgrundlage zur Videoüberwachung durch öffentliche Stellen (in Wahrnehmung des Hausrechts bzw. soweit zur Aufgabenerfüllung der verantwortlichen Stellen erforderlich) in § 34 SDSG ausgesprochen.

Die vorgenommene weite gesetzliche Öffnung zum Einsatz der Videotechnik wird dem Gebot der Datenvermeidung und Datensparsamkeit nicht gerecht (§ 4 Abs. 4 SDSG). Eine derartige ausgestaltete Legalisierung des Videoeinsatzes für die öffentlichen Stellen kann und wird den Anreiz dazu geben, alternative, die Grundrechte weniger belastende Methoden zur Beseitigung von Alltagsproblemen nicht mehr näher in Betracht zu ziehen und dies regelmäßig nur aus Kostengründen. Dies kann schon in Anwendung der in Nr. 1 vorgesehenen Bestimmung der Fall sein, wenn zur vorgeblichen Wahrung des Hausrechts Videokameras installiert werden, die nur dann eine Präventionswirkung entfalten könnten, wenn entsprechendes Personal zum Eingreifen bereit stehen würde. Das zeitliche Erkennen von Gefahrensituationen und das gleichzeitige Beheben dieser durch eine einzige, vor einem weit entfernten Monitor eingesetzte Person kann nur schwerlich erfolgen.

Zu bedenken wäre ebenfalls gewesen, dass das Hausrecht nur in seltenen Ausnahmefällen missachtet wird, bei der Videoüberwachung aber eine weit überwiegende Anzahl unbeteiligter Personen beobachtet wird, ohne dass diese zu einer Gefahrenlage auch nur das Geringste beigetragen haben bzw. jemals beitragen werden.
Aus der Sicht des Datenschutzes wird die Legalisierung des Einsatzes von Videotechnik für öffentliche Stellen – betrachtet man zudem die vorstellbaren Anwendungsfälle – für die Bevölkerung keinen objektiven Sicherheitsgewinn bewirken, sondern nur Verlagerungseffekte bedingen.
Ich werde jedenfalls gemäß § 7 Abs. 2 SDSG die zukünftige erstmalige Einführung jeglicher Videoüberwachungsvorrichtungen durch öffentliche Stellen aufmerksam verfolgen.

5 Verfassungsschutz

5.1 Prüfung des Landesamtes für Verfassungsschutz

Das Landesamt für Verfassungsschutz (LfV) wurde in den Monaten Juni und Juli 2006 einer Querschnitt-Prüfung unterzogen. Nach dem Zufallsprinzip wurden Sachakten aus allen Arbeitsbereichen des Verfassungsschutzes gezogen und durch mein Fachreferat überprüft.
Erfreulicherweise wurden weder im fachlichen Bereich noch im technisch-organisatorischen Umfeld wesentliche Mängel festgestellt.

5.2 Verwaltungsvereinbarung zwischen dem Landeskriminalamt (LKA) und dem Landesamt für Verfassungsschutz (LfV) über die Bereitstellung und Nutzung von Aufzeichnungstechnik im G 10 -Bereich

Im Rahmen der Amthilfe begehrte das LfV bei Überwachungsmaßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel10-Gesetz – G 10) aus Gründen der Wirtschaftlichkeit und Sparsamkeit die beim LKA vorhandene Aufzeichnungstechnik mitzubenutzen, weswegen meiner Dienststelle seitens des Ministeriums für Inneres, Familie, Frauen und Sport der entsprechende Entwurf einer Verwaltungsvereinbarung zwischen dem LKA und dem LfV vorgelegt wurde. Da es sich hier aber um Telefonüberwachungsmaßnahmen im G 10 - Bereich handeln sollte, obliegt die Kontrolle der gesamten Erhebung, Verarbeitung und Nutzung der nach Artikel 10-Gesetz erlangten personenbezogenen Daten des LfV gemäß § 3 Abs.4 Satz 2 des G 10-Durchführungsgesetzes ausschließlich der G 10-Kommission. Ich habe daher empfohlen, die G 10-Kommission einzuschalten und ein Sicherungskonzept hinsichtlich der Trennung der Datenbestände des LKA gegenüber dem LfV angefordert, welches mir sodann seitens des LKA übersandt wurde.

Aus datenschutzrechtlicher Sicht ergeben sich hierfür keine Beanstandungen.

6 Steuern

6.1 Parkkralle

Bereits in meinem 17. Tätigkeitsbericht hatte ich mich mit der Zulässigkeit des Einsatzes der Parkkralle zur Beitreibung rückständiger Abgaben auseinandergesetzt und betont, dass bei Wahrung datenschutzrechtlicher Gesichtspunkte und unter Einhaltung der vollstreckungsrechtlichen Voraussetzungen gegen den Einsatz der Parkkralle keine grundsätzlichen Bedenken bestehen.

Durch Feststellungen in anderen Bundesländern wurde bekannt, dass die Vollstreckungsstellen der Finanzämter aufgrund einer Dienstanweisung Mitteilungen an die Ordnungsämter und die Polizei über blockierte Fahrzeuge zukommen lassen. Hierbei übermitteln Sie den Namen des Fahrzeughalters, das Kfz-Kennzeichen, den Standort und die Tatsache, dass Steuerschulden vorliegen.

Aus datenschutzrechtlicher Sicht stellt sich die Frage, ob die mit der Mitteilung an die Ordnungsbehörden verbundene Offenbarung persönlicher Daten aus straßenverkehrsrechtlicher Sicht überhaupt erforderlich und damit zulässig ist.

Das Ministerium für Inneres, Familie, Frauen und Sport (MfIFFS) hat mir mitgeteilt, dass das Blockieren eines im öffentlichen Verkehrsraum geparkten Fahrzeuges grundsätzlich eine über den Gemeingebrauch hinausgehende Sondernutzung bewirkt, die nach §18 Saarländisches Straßengesetz der Erlaubnis der zuständigen Straßenbaubehörde bedarf. Somit wird die Erforderlichkeit der Mitteilung bejaht.

Nach Ansicht des MfIFFS genügt jedoch die Nennung von Fahrzeugart, Örtlichkeit und Dauer der Blockierung. Die Übermittlung personenbezogener Daten wird nicht für erforderlich gehalten.

Aufgrund dieser Stellungnahme hat das Ministerium der Finanzen einer datenschutzfreundlicheren Vorgehensweise zugestimmt und die Vollstreckungsstellen angewiesen keine personenbezogenen Daten mehr zu übermitteln.

7 Wahlen

7.1 Melderegisterauskünfte an Parteien

Durch eine Eingabe wurde ich darüber informiert, dass aus Anlass einer Bürgermeisterwahl mit einem sehr großen Adressbestand Wahlwerbung betrieben wurde. Die Art der Wahlwerbebriefe legte den Verdacht nahe, dass in unzulässiger Weise Meldedaten an die Partei einer/eines Bürgermeisterkandidatin/en geliefert wurden. Aufzeichnungen über Art und Umfang der gelieferten Daten waren beim Meldeamt der Gemeinde nicht geführt worden.

Aufgrund von Nachforschungen (Untersuchung einer Festplatte auf Fragmente gelöschter Dateien) konnte festgestellt werden, dass durch das Meldeamt der Kommune Dateien mit den Gruppenmerkmalen verschiedener Jahrgangsgruppen erstellt wurden (Erstwähler, verschiedene Seniorengruppen). Aus vorliegenden Wahlwerbebriefen ging weiterhin hervor, dass auch Personengruppen angeschrieben wurden, die eine außerdeutsche Staatsangehörigkeit besaßen, und die deshalb in Ihrer Heimatsprache angesprochen wurden.

Die ausschließliche Rechtsgrundlage für eine zulässige Auskunft an Parteien aus dem Melderegister über Wahlberechtigte ist in § 35 Meldegesetz enthalten. Da es sich datenschutzrechtlich um eine Datenübermittlung an eine nichtöffentliche Stelle handelt, hat der Gesetzgeber zum Schutz des Rechts auf informationelle Selbstbestimmung mehrere Voraussetzungen festgelegt, die zu beachten sind.

Als grundlegende Voraussetzung muss die Meldebehörde nach § 35 Absatz 4 Meldegesetz die Wahlberechtigten durch öffentliche Bekanntmachung acht Monate vor der Wahl auf das Widerspruchsrecht gegen die Übermittlung ihrer Daten hinweisen.
Diese Bekanntmachung war im vorliegenden Fall unterblieben. Somit konnte sich die Gemeinde nur rechtmäßig verhalten, indem sie generell eine Datenübermittlung an die Parteien unterlässt.

Die Parteien erhalten auch nur Daten von Gruppen, für deren Zusammensetzung das Lebensalter entscheidend ist. Eine Gruppenauswahl nach Geschlecht oder Staatsangehörigkeit, wie sie vorliegend vermutet werden kann, ist unzulässig.

Der Datenschutzverstoß wurde von mir gemäß § 27 Absatz 1 SDSG förmlich beanstandet.
Die Gemeinde hat mittlerweile eine „Dienstanweisung zur Behandlung von Anfragen bei der Meldebehörde über Wahlberechtigte im Zusammenhang mit allgemeinen Wahlen gemäß § 35 Meldegesetz“ erstellt.

Durch Urteil des Verwaltungsgerichts des Saarlandes wurde die Kommunalaufsichtsbehörde verpflichtet, die Bürgermeisterwahl wegen Verstoßes gegen eine Datenschutzbestimmung – als gleichzeitig wesentliche Wahlvorschrift – für ungültig zu erklären. Gegen das Urteil wurde Berufung eingelegt.

7.2 Internetveröffentlichung von Wahlbewerbern und gewählten Wahlbewerbern

Ein Mitglied eines Ortsrates beschwerte sich darüber, dass im Internetangebot des Statistischen Landesamtes personenbezogene Daten von ihm veröffentlicht waren, und zwar Name, Parteizugehörigkeit, Listenplatz und Ort bzw. Ortsteil. Da er sein Recht auf informationelle Selbstbestimmung berührt sah, bat er um Löschung dieser Daten.

Das Ministerium für Inneres als zuständige Aufsichtsbehörde des Statistischen Landesamtes hielt die Veröffentlichung durch das Statistische Landesamt für zulässig. Die Daten seien aufgrund der Vorschriften des Wahlgesetzes durch die Gemeinden in der lokalen Presse veröffentlicht worden und somit in allgemein zugänglichen Quellen publiziert. Entgegenstehende berechtigte Interessen der Wahlbewerber seien aufgrund der Öffentlichkeit der Wahlbewerbung und Wahldurchführung nicht ersichtlich. Daraufhin verweigerte das Statistische Landesamt eine Löschung der Daten.

Weiter wurde mir mitgeteilt, dass für die aus der Kommunalwahl resultierenden Veröffentlichungen der Gemeindewahlleiter als verantwortliche Stelle im Sinne des § 3 Absatz 3 Saarländisches Datenschutzgesetz zuständig ist. Mithin wurde das Statistische Landesamt in Auftragsdatenverarbeitung tätig und der Gemeindewahlleiter war für Art und Umfang der Datenverarbeitung zuständig.

Das Kommunalwahlgesetz sieht eine Veröffentlichungsbefugnis lediglich für eine ortsübliche Bekanntmachung vor (§§ 45, 98 KWG i.V.m. Verordnung über die öffentlichen Bekanntmachungen der Gemeinden und Gemeindeverbände - Bekanntmachungsverordnung BekVO). Diese Rechtsgrundlagen erlauben jedoch keineswegs den qualitativen Sprung einer weltweiten Veröffentlichung im Internet.

Bei der Wahl des Veröffentlichungsmediums muss die strenge Erforderlichkeit zur Aufgabenerfüllung der Behörde noch erkennbar sein. Eine globale Verfügbarkeit von Daten steht im krassen Gegensatz zu der lokalen Begrenzung des Aufgaben- und Wirkungskreises einer Kommune. Es ist nicht die Aufgabe einer Kommune den Internetnutzern auf der ganzen Welt frei Haus Informationen über Vorgänge in ihrem Bereich zu liefern, noch haben Internetnutzer ein generelles berechtigtes Interesse an solchen Informationen.

Der Gemeindewahlleiter teilte meine Auffassung und wies das Statistische Landesamt an, den Datensatz zu löschen.

Damit war die Informationsquelle im Internet beseitigt, was jedoch blieb, waren die Einträge in den Suchmaschinen von Google und Yahoo. Die personenbezogenen Daten des Ortsratsmitgliedes wurden weiterhin in Trefferlisten angezeigt, der entsprechende Link zur Seite des Statistischen Landesamtes führte aber bereits ins Leere.
Auf meinen entsprechenden Hinweis an die Suchmaschinenbetreiber, verbunden mit der Bitte die personenbezogenen Daten des Ortsratsmitgliedes in den Trefferlisten zu löschen, wurden dankenswerterweise umgehend reagiert.

7.3 Wahlwerbebriefe an Bedienstete einer Kommune

Im Vorfeld der Bürgermeisterwahlen in einer saarländischen Kommune wurden persönliche Anschreiben an die Bediensteten der Kommune versandt mit der Aufforderung eine bestimmte Person zu unterstützen. In Zusammenarbeit mit der für den privaten Bereich zuständigen Datenschutzaufsicht beim Ministerium des Innern konnte festgestellt werden, dass die Adressdaten unter anderem aus internen Telefonlisten der Kommune stammten, die mit einer entgeltlich erworbenen Liste des externen Dienstleisters abgeglichen wurden, der die Gehaltsabrechnungen der kommunalen Bediensteten erstellte. Die Daten waren auf Anforderung des Wahlkampfbüros den Wahlbewerbern geliefert worden.

Die Verarbeitung personenbezogener Daten ist gemäß § 4 SDSG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Beide Voraussetzungen waren nicht erfüllt.

Die Datenübermittlung durch den externen Dienstleister erfolgte ohne Wissen der Personalabteilung der Kommune. Eine selbständige Verarbeitung einer Anfrage für Personaldaten ist aber mit der Auftragnehmerstellung des Dienstleisters nicht vereinbar. Ein Auftragnehmer darf personenbezogene Daten nur im Rahmen des vertraglich Festgelegten verarbeiten (§ 5 Absatz 1 SDSG).

Die Kommune wurde aufgefordert insbesondere gegenüber dem externen Dienstleister Maßnahmen zu ergreifen, die einen Datenschutzverstoß in der Zukunft ausschließen.

8 Meldewesen

8.1 Meldedatenübermittlungsverordnung

Das Meldegesetz wurde mit Wirkung vom 23.12.2005 neu gefasst. Hierbei standen die schnellere Aktualisierung der Melderegister im informationstechnischen Bereich und die Automatisierung des Datenaustausches im Vordergrund. Dies bedingte eine Überarbeitung der Meldedatenübermittlungsverordnung, die sich mit der Datenübermittlung aus dem Melderegister befasst. Es wurde mir daher ein erster Vorabentwurf dieser Verordnung im September 2006 übersandt. Bereits dieser erste Entwurf ließ eine erhebliche Ausweitung der regelmäßigen Datenübermittlung aus dem Meldregister und des automatisierten Abrufverfahrens und dies weitgehend ohne hinreichende bzw. nachvollziehbare Begründung erkennen.

Mit Schreiben vom 26.01.2007 wurde mir sodann im Rahmen des externen Anhörungsverfahrens ein neuerlicher Entwurf einer Verordnung über die Zulassung der regelmäßigen Übermittlung von Daten aus dem Melderegister an Behörden oder sonstige Stellen (MeldDÜV) mit der Bitte um Stellungnahme übersandt.

Im Einzelnen bemerke ich besonders:

§ 3 der MeldDÜV regelt die Datenübermittlung an Sicherheitsbehörden. Nach Absatz 2 dieser Vorschrift dürfen Abfragen von Sicherheitsbehörden melderegisterübergreifend und als Gruppenabfrage durchgeführt werden. Die durch diese Vorschrift eröffneten Möglichkeiten berücksichtigen weder die Grundsätze der Datensparsamkeit noch die der Verhältnismäßigkeit und sind meines Erachtens daher eindeutig überzogen. Aufgrund meiner Stellungnahme konnte ich im weiteren Gesetzgebungsverfahren wenigstens eine bescheidene Konkretisierung der Abfrage durch Eingabe weiterer Merkmale erreichen, die ursprünglich erst bei einer Trefferzahl von 200 Personen vorgesehen war und nunmehr auf eine Trefferzahl von 100 Personen begrenzt wurde.

Bei der Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften nach § 9 MeldDÜV wurde seitens des Gesetzgebers meinem Vorschlag gefolgt, die Terminologie des § 32 Abs.1 Nr.11 Saarländisches Meldegesetz wortgleich zu übernehmen, um einen gegensätzlichen Rechtscharakter zu vermeiden.

Auch meiner Forderung auf die Datenübermittlung des Ein- und Auszugstages schulpflichtiger Kinder an Grundschulen, mangels Notwendigkeit, zu verzichten, wurde in der derzeit gültigen Fassung des § 10 MeldDÜV Rechnung getragen.

§ 18 Absatz 2 MeldDÜV regelt das Abrufverfahren für Gerichte. Die Zulässigkeitsvoraussetzungen dieser Norm wurden nach meiner Auffassung nicht hinreichend definiert. Darüber hinaus erscheint fraglich, ob der im Abrufverfahren übermittelte Informationsgehalt aufgrund fehlender Eilbedürftigkeit für besagte Stellen stets bereitgehalten werden muss. Hierfür hält das Melderecht andere Instrumentarien (Melderegisterauskunft) bereit.

Die in den §§ 24 bis 37 MeldDÜV geregelte Datenübermittlung in automatisierter Form räumt nunmehr die Möglichkeit ein, an zusätzliche Daten des Betroffenen zu gelangen, ohne dass, wie von mir postuliert, das datenschutzrechtliche Primat der „Datenerhebung beim Betroffenen“ oder zumindest eine Beschränkung auf die Grunddatenerhebung beachtet wurde.

Bedauerlicherweise musste ich nach der Veröffentlichung der Meldedatenübermittlungsverordnung im Amtsblatt des Saarlandes vom 08. Juni 2007 feststellen, dass zwei weitere Vorschriften, nämlich § 15 (Datenübermittlung an Jugendämter) und § 33 (Abrufverfahren für die Sozialämter) in das Gesetzeswerk ohne die Beteiligung meiner Dienststelle eingearbeitet wurden.

Abschließend möchte ich daher festhalten, dass die Meldedatenübermittlungsverordnung in Ihrer derzeit gültigen Fassung eine erhebliche Ausweitung der regelmäßigen Datenübermittlung darstellt, wobei der Verordnungsgeber hier seiner Begründungspflicht nur äußerst spärlich nachkam.

9 Kommunales

9.1 Parkgebühren zahlen mit dem Handy

Unterstützt durch das Innen- und finanziell gefördert durch das Wirtschaftsministerium wurde im Jahr 2005 in den Städten Neunkirchen und Saarbrücken ein System zur Zahlung der Parkgebühren über das Handy eingeführt. Über das Vorhaben wurde ich zwar nicht frühzeitig, aber dennoch rechtzeitig informiert um es datenschutzrechtlich zu begleiten.

Betreiber des Systems ist eine saarländische Firma. Der Verkehrsteilnehmer, der das System nutzen will, meldet sich über Internet beim Betreiber an. Der Betreiber speichert Name, Vorname, Adresse, Handynummer, Kfz-Kennzeichen, Bankverbindung, sowie einen Benutzernamen und eine PIN. Diese Daten werden einerseits für die Abrechnung der Parkgebühren benötigt und andererseits um den städtischen Parkraumkontrolleuren anzuzeigen, ob ein Kfz im System als parkend eingebucht ist. Bei einem Parkvorgang ruft der Nutzer mit seinem Handy eine in der Parkzone angegebene Nummer an und erhält eine Bestätigungs-SMS. Diesen Vorgang muss er wiederholen, wenn er die Parkzone verlässt.

Aus durchaus nachvollziehbaren Gründen wollte der Betreiber die persönlichen Daten der Nutzer auch für Zwecke kommerzielle Natur verwenden. Unter anderem wurde der Versand von Werbenachrichten per SMS genannt.

Da der Parkende jedoch ausschließlich in eine Rechtsbeziehung zu der Kommune eintritt, die den Parkraum zu verwalten hat, bleibt die Kommune alleine Herr der Daten. Nichtöffentliche Stellen können im vorliegenden Fall lediglich als unselbständige Verwaltungshelfer ohne eigene Entscheidungskompetenz gegenüber dem Parkenden mit technisch-organisatorischen Hilfstätigkeiten betraut werden. Aus Sicht des Datenschutzes war mit dem Betreiber ein Vertrag zur Auftragsdatenverarbeitung abzuschließen, der den Auftragnehmer nicht dazu legitimiert im Rahmen eines öffentlich-rechtlichen Vorgangs parallel eine nicht weisungsgebundene private Rechtsbeziehung zu eröffnen.

Dieser Auffassung haben sich die betroffenen Kommunen angeschlossen und sind entsprechende Verträge zur Auftragsdatenverarbeitung mit dem Betreiber eingegangen.

9.2 Videoüberwachung von Müllcontainern durch eine Kommune

Bereits im Februar 2004 hatte ich durch Presseveröffentlichungen erfahren, dass in einer saarländischen Gemeinde die Videobeobachtung der Müllcontainer in Erwägung gezogen werde. In einem an den Bürgermeister gerichteten Schreiben wies ich darauf hin, dass im Saarland für dieses Vorhaben eine gesetzliche Grundlage fehlt und bat, von der geplanten Maßnahme abzusehen.

Eine personenbezogene Videoüberwachung stellt einen tiefen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der nur auf Grund eines Gesetzes im überwiegenden Interesse der Allgemeinheit zulässig ist.

Im August 2006 berichtete der Saarländische Rundfunk (SR1) über durchgeführte Videoüberwachungen der Müllcontainer in dieser Gemeinde. Der Bürgermeister sprach dabei von einem dreimonatigen, erfolgreichen Test. In dieser Zeit seien Personen ermittelt worden, denen ein Bußgeld auferlegt worden sei.

Da es sich um einen bewussten und gravierenden Datenschutzverstoß handelte, habe ich die Vorgehensweise nach § 27 Saarländisches Datenschutzgesetz unter gleichzeitiger Unterrichtung der für die Stadt zuständigen Aufsichtsbehörde beanstandet.

10 Soziales

10.1 Hartz IV

Ein Schwerpunktthema in meiner Dienststelle waren datenschutzrechtliche Probleme im Zusammenhang mit der Umsetzung von Hartz IV. Neben einer Reihe von Petitionen, die ich in diesem Zusammenhang zu bearbeiten hatte, mussten sich der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz mit gravierenden grundsätzlichen Problemen beschäftigen.

So mussten verschiedene Landesbeauftragte für den Datenschutz erleben, dass ihnen von den zuständigen ARGE'n das Recht abgesprochen wurde, ihre Dienststellen zu kontrollieren. Es wurde argumentiert, dass wegen der geteilten Zuständigkeiten innerhalb der ARGE'n (die Bundesagentur als Trägerin der Leistungen zur Eingliederung in Arbeit und der Geldleistungen zur Sicherung des Lebensunterhaltes, die Kommunen als Leistungsträger für die Kosten der Unterkunft und Heizung) eine geteilte Kontrollkompetenz zwischen dem Bundesbeauftragten für den Datenschutz und den Landesbeauftragten für den Datenschutz bestehe. Dem steht gegenüber, dass der Gesetzgeber den ARGE'n diese Aufgaben zur einheitlichen Wahrnehmung übertragen hat; die ARGE'n sind berechtigt, zur Erfüllung ihrer Aufgaben Verwaltungsakte und Widerspruchsbescheide zu erlassen.

Auf ihrer 72. Konferenz am 26./27. Oktober 2006 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgenden Beschluss gefasst:

1. Die Kontrollkompetenz der LfD bezieht sich auf alle Leistungen nach dem SGB II.
2. Die ARGE'n sind unmittelbar Adressaten von eventuellen Beanstandungen der LfD. In Fällen grundsätzlicher Art sollte der BfDI über Beanstandungen informiert werden.
3. Auch wenn der BfDI Kontrollstelle für die zentralen IT-Verfahren der BA ist, sind die ARGE'n verpflichtet, den LfD Einblick in oder Auskunft über die technischen Verfahren zu geben, die zu bestimmten Beschwerden Anlass geben. Entsprechendes gilt auch für die Hinweise zu Verfahren, Empfehlungen usw. der BA. Die LfD können diese Verfahren/Hinweise selbst nicht datenschutzrechtlich bewerten, aber sie müssen diese zur Kontrolle der datenschutzge-

mäßen Aufgabenerledigung der ARGE'n direkt (vor Ort) zur Kenntnis nehmen können.

4. Die Bestellung von behördlichen Datenschutzbeauftragten in den ARGE'n richtet sich nach Landesrecht.
5. Im Einzelfall können sich die LfD auch direkt an die BA wenden.

Das Bundesministerium für Arbeit und Soziales trägt diesen Beschluss mit, die Bundesagentur für Arbeit hat die Regionaldirektionen und die ARGE'n auf diese Datenschutzkontrollzuständigkeiten und die damit verbundenen Rechte und Pflichten hingewiesen. Das saarländische Ministerium für Wirtschaft und Arbeit teilt ebenfalls die Auffassung der Datenschutzbeauftragten und hat zugesagt, im Rahmen seiner Rechtsaufsicht über die ARGE'n darauf hinzuwirken, dass wir unsere Befugnisse innerhalb der ARGE'n ordnungsgemäß ausüben können.

Bereits in meinem letzten Tätigkeitsbericht hatte ich auf datenschutzrechtliche Defizite beim Umfang der Antragsvordrucke sowie bei der für die Leistungsberechnung eingesetzten Software A2LL hingewiesen.
In einer Entschließung vom 27./28.10.2005 (Anlage 17.7) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder noch einmal kritisiert, dass für die Leistungsberechnungssoftware kein klar definiertes Zugriffsberechtigungskonzept umgesetzt ist und dass eine Protokollierung der lesenden Zugriffe nicht erfolgt. Damit sei es über 40000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und –empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.
Mittlerweile hat die Bundesagentur für Arbeit ein Berechtigungskonzept vorgelegt, in dem umfassend beschrieben ist, welche Personenkreise auf welche Daten zugreifen dürfen.
Vorgelegt wurde außerdem von der Bundesagentur für Arbeit ein Konzept zur Protokollierung von Suchanfragen in dem System. Dieses Konzept enthält insbesondere Aussagen zur Aufbewahrungsdauer der Protokolldaten und zum Auswerte- bzw. zum Löschungsverfahren.
Es kommt nun darauf an, dass diese Konzepte im System implementiert werden; die Datenschutzbeauftragten werden die Entwicklung beobachten.

Die Antragsvordrucke wurden unter Beteiligung des Bundesbeauftragten und der Landesbeauftragten für Datenschutz umfassend überarbeitet. Bis auf einige Detailfragen sind die entsprechenden Vordrucke nunmehr im Wesentlichen als datenschutzgerecht zu bezeichnen. Wenn den Betroffenen zusätzlich die ergänzenden neuen Ausfüllhinweise übergeben werden, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit die Erhebung von nicht erforderlichen Daten vermieden.

Für bundesweites Aufsehen hat es gesorgt, als die Bezieher von Arbeitslosengeld II im Jahre 2005 von einem privaten Callcenter angerufen und nach Sozialdaten im Zusammenhang mit ihrem Antrag auf Arbeitslosengeld II gefragt wurden.
Es stellte sich heraus, dass die Bundesagentur für Arbeit dieses Callcenter beauftragt hatte, einen Abgleich von Daten vorzunehmen, da die vorhandenen Datensätze nicht immer vollständig waren.
Auch wenn im Grundsatz die Beauftragung eines Dritten mit der Erhebung von Daten nicht zu beanstanden ist, so musste an der Art der Durchführung der Befragungsaktion deutliche Kritik geübt werden.
Unverzichtbar wäre eine vorherige schriftliche Information der Betroffenen gewesen. Eine solche Information hätte es den Betroffenen ermöglicht, sich nach reiflicher Überlegung für oder gegen eine Teilnahme zu entscheiden. Denn eine Verpflichtung, sensible Sozialdaten am Telefon zu offenbaren, besteht nicht. Dementsprechend hätte in der Vorabinformation ausdrücklich auf die Freiwilligkeit und die Möglichkeit, sich stattdessen an seine zuständige ARGE zu wenden, hingewiesen werden müssen.
Diese Auffassung haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 27./28.10.2005 (Anlage 17.7) bekräftigt und die Verantwortlichen dazu aufgefordert, die Sach- und Rechtslage klarzustellen und bei bereits angekündigten neuen Telefonaktionen eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.
Soweit ersichtlich, wurden die Forderungen bei nachfolgenden Telefonaktionen berücksichtigt.

10.2 Auskunftspflicht des Ehegatten des Unterhaltspflichtigen bei Sozialhilfegewährung

Ein Bürger hat sich mit folgender Anfrage an meine Dienststelle gewandt:
Seine Schwiegermutter ist auf Kosten der Sozialhilfe in einem Altenheim untergebracht. Vom Sozialamt wurde er aufgefordert, eine Erklärung über seine wirtschaftlichen Verhältnisse abzugeben, also Angaben zu seinem Einkommen und Vermögen zu machen.
Der Petent bezweifelt, dass er verpflichtet ist, diese Angaben zu machen, da ein Unterhaltsrechtsverhältnis nur zwischen seiner Ehefrau und deren Mutter bestehe und er rechtlich nicht verpflichtet sei, zu dem Unterhalt der Mutter seiner Ehefrau beizutragen. Er wollte darüber hinaus wissen, ob er, wie vom Sozialamt verlangt, Einzelbelege vorlegen müsse, wie Rentenbescheide, Kontoauszüge usw.

Während in der Vergangenheit streitig war, ob eine Auskunftspflicht des Ehegatten des Unterhaltspflichtigen gegenüber dem Sozialamt besteht, ist diese Frage nunmehr durch eine Änderung der sozialhilferechtlichen Vorschriften geklärt. Gemäß § 117 SGB XII sind die Unterhaltspflichtigen sowie ihre nicht getrennt lebenden Ehegatten oder Lebenspartner gegenüber dem Träger der Sozialhilfe zur Auskunft über ihre Einkommens- und Vermögensverhältnisse verpflichtet, soweit es die Durchführung der Sozialhilfe erfordert.
In mehreren Urteilen wurde höchstrichterlich festgestellt, dass das Einkommen des Ehegatten bei der Ermittlung der Unterhaltspflicht zu berücksichtigen ist.
Auch wenn die Träger der Sozialhilfe grundsätzlich die Vorlage von Beweisurkunden verlangen dürfen, habe ich dem Sozialamt in dem konkreten Fall empfohlen, auf die Anforderung von detaillierten Belegen zu verzichten, wenn die Angaben plausibel erscheinen und nicht zu erwarten ist, dass ein Unterhaltsbeitrag in Betracht kommt.

10.3 Datenerhebung des Jugendamtes beim Arbeitgeber eines Unterhaltsverpflichteten

Der Vater eines Kindes, der von seiner Ehefrau geschieden ist, beschwerte sich bei meiner Dienststelle, dass sich das Jugendamt als Beistand des Kindes an seinen

Arbeitgeber gewandt habe, um Auskunft über seine Einkünfte zu erhalten. Der Petent meint, er habe seine Auskunftspflicht bereits dadurch erfüllt, dass er der Prozessbevollmächtigten seiner geschiedenen Ehefrau vollständig Auskunft über sein Einkommen erteilt habe; die Frist des § 1605 Absatz 2 BGB, wonach grundsätzlich vor Ablauf von 2 Jahren nicht erneut Auskunft verlangt werden kann, sei noch nicht abgelaufen.

Durch das am 1. Juli 1998 in Kraft getretene Beistandsgesetz wurde die Beistandschaft als allgemeines Rechtsinstitut für allein erziehende Elternteile eingeführt (§ 1712 ff BGB). Aufgabe des Beistandes kann es sein, den Unterhaltsanspruch des Kindes gegen den unterhaltspflichtigen Elternteil geltend zu machen. Der Mitarbeiter des Jugendamtes, dem die Ausübung der Beistandschaft übertragen wird, wird damit zum gesetzlichen Vertreter des Kindes (§ 55 Absatz 2 SGB VIII).

Gemäß § 1605 BGB ist der unterhaltspflichtige Vater gegenüber dem Kind verpflichtet, über seine Einkünfte und sein Vermögen Auskunft zu erteilen und auf Verlangen Belege, insbesondere Bescheinigungen des Arbeitgebers vorzulegen. Die Erfüllung dieser Auskunftspflicht ist gegenüber dem nichtehelichen Vater einklagbar. Die gesetzlichen Bestimmungen bieten keinen Anhaltspunkt dafür, dass das Jugendamt als Beistand über besondere „amtliche“ Befugnisse verfügt. Insbesondere besteht keine – etwa der Regelung des § 97a SGB VIII vergleichbare – gesetzliche Auskunftspflicht des Arbeitgebers gegenüber dem Jugendamt. Das Jugendamt wird vielmehr gegenüber dem Vater und dem Arbeitgeber wie ein Privater als gesetzlicher Vertreter des Kindes tätig.
Den Auskunftsanspruch kann der Beistand dadurch realisieren, dass er die Vorlage von Verdienstbescheinigungen verlangt. Kommt der Unterhaltspflichtige diesem Verlangen nicht nach, kann der Anspruch auf Herausgabe der Verdienstbescheinigungen gerichtlich durchgesetzt werden.
Bei dieser Verfahrensweise wird einerseits vermieden, dass der Arbeitgeber erfährt, dass sein Arbeitnehmer Kontakt mit dem Jugendamt hat, wobei auch der Eindruck entstehen kann, dieser wolle gesetzlichen Verpflichtungen nicht nachkommen. Andererseits ist eine Auskunftsverpflichtung nicht in jedem Fall zweifelsfrei gegeben, wie der vorliegende Fall zeigt, in dem sich der Petent darauf beruft, dass er erst nach

Ablauf von zwei Jahren zur erneuten Auskunft verpflichtet sei; diese Frage kann im familiengerichtlichen Verfahren zunächst geklärt werden.

Ich habe das zuständige Jugendamt aufgefordert, diesen Fall zum Anlass zu nehmen, seine Mitarbeiter darauf hinzuweisen, dass im Rahmen einer Beistandschaft grundsätzlich Verdienstanfragen beim Arbeitgeber datenschutzrechtlich nicht zulässig sind.

10.4 Einsicht in Umgangsrechtsakten des Jugendamtes

Immer wieder beschweren sich Bürger bei meiner Behörde darüber, dass ihnen von Behörden Einsicht in die sie betreffenden Akten verwehrt wird. Dies liegt nach meinem Eindruck meist darin begründet, dass bei den Behördenmitarbeitern die datenschutzrechtlichen Auskunftsansprüche nicht hinreichend bekannt sind.
So offensichtlich auch in dem Fall, den ich nachstehend schildern möchte:
Eine Mutter wollte die Frage des Umgangsrechtes mit ihrem Sohn einer Klärung zuführen, nachdem es diesbezüglich zu Problemen zwischen ihr und dem Kindesvater gekommen war. Vor einer eventuellen gerichtlichen Geltendmachung ihres Anspruches eines Umgangsrechtes wollte sie Akteneinsicht in die Umgangsrechtsakte des Jugendamtes nehmen, das beratend für die Eltern tätig war.
Die beantragte Akteneinsicht wurde von dem betreffenden Jugendamt mit der pauschalen Begründung abgelehnt, dass das Jugendamt im Rahmen seiner Beratungstätigkeit für Familien grundsätzlich keine Akteneinsicht gewähre.
Ich habe folgende Rechtsauffassung vertreten: Gemäß § 83 SGB X ist dem Betroffenen auf Antrag grundsätzlich Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Die Auskunftserteilung darf unter bestimmten Voraussetzungen unterbleiben, etwa wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen (§ 83 Absatz 4 SGB X).
Ich habe das betreffende Jugendamt darauf hingewiesen, dass jedenfalls die pauschale Begründung, im Rahmen einer Beratungstätigkeit für Familien grundsätzlich keine Akteneinsicht zu gewähren, als Grund für die Verweigerung der Akteneinsicht

nicht ausreicht. Vielmehr ist in jedem Einzelfall zu begründen, aus welchem Grund eine Akteneinsicht nicht gewährt wird.
Meine Intervention hat dazu geführt, dass der Mutter die gewünschte Akteneinsicht gewährt wurde.

Hinweisen möchte ich noch darauf, dass nach meiner Auffassung dem Auskunftsbegehren regelmäßig durch Gewährung von Akteneinsicht entsprochen werden muss, auch wenn § 83 SGB X dies so nicht ausdrücklich regelt, sondern von „Auskunftserteilung“ spricht. Ich meine, dass die Akteneinsicht regelmäßig das adäquateste Mittel zur Verwirklichung des Rechts auf informationelle Selbstbestimmung ist, da der Bürger so am zuverlässigsten erfahren kann, über welche Informationen eine Behörde über seine Person verfügt. Die Ermessensentscheidung, die § 83 Absatz 4 Satz 1 SGB V den Sozialbehörden bei der Entscheidung über die Art und Weise der Auskunftserteilung einräumt, ist, soweit der Antragsteller dies wünscht, regelmäßig dahingehend zu treffen, dass Akteneinsicht gewährt wird.

10.5 Amtshilfeersuchen gegenüber Finanzamt

Als ein Bezieher von Arbeitslosengeld II Einsicht in seine Akte bei der ARGE nahm, stieß er auf ein Schreiben an das für ihn zuständige Finanzamt, in dem das Finanzamt gebeten wurde, den Gewinn mitzuteilen, den der Gewerbebetrieb des Betroffenen in den letzten Jahren abgeworfen habe. Der Betreffende habe bei der Antragstellung verschwiegen, dass er Inhaber eines Gewerbebetriebes sei; es bestehe der Verdacht des Sozialleistungsbetruges.
Empört wandte sich der Petent an meine Dienststelle. Er verwahrt sich gegen den Vorwurf des Sozialleistungsbetruges, er habe stets alle Daten korrekt angegeben.
Folgenden Sachverhalt konnte ich feststellen: Der Petent hatte in seinem Antrag auf Arbeitslosengeld II als Art seiner selbständigen Tätigkeit angegeben: „Übersetzer/Dolmetscher, Verlagswesen“. Der Petent wollte damit zum Ausdruck bringen, dass er Übersetzer und Dolmetscher ist und außerdem eine Tätigkeit im Verlagswesen ausübt. Die ARGE hat diese Angabe dagegen so verstanden, dass der Petent Übersetzer und Dolmetscher im Verlagswesen sei. Nachdem sie von dritter Seite einen Hinweis erhalten hatte, dass der Petent Inhaber eines Gewerbebetriebes im

Bereich der Herstellung von Druckerzeugnissen sei, wollte sie mit Hilfe des Finanzamtes die Gewinne dieses Betriebes in Erfahrung bringen.
Ich halte diese Verfahrensweise der ARGE für datenschutzrechtlich nicht zulässig. Selbst wenn die ARGE der Meinung war, der Petent habe in seinem Antrag eine Tatsache verschwiegen, wäre es erforderlich gewesen, vor eine Anfrage bei dem Finanzamt die aus ihrer Sicht bestehende Unsicherheit durch eine Rückfrage bei dem Petenten zu klären. Gemäß § 21 Absatz 4 SGB X sind die Finanzbehörden zur Auskunft über die ihnen bekannten Einkommensverhältnisse eines Sozialleistungsbeziehers nur insoweit befugt, wie es in einem Sozialleistungsfall erforderlich ist.
Die ARGE hätte ihr Ziel auch dadurch erreichen können, dass sie den Antragsteller selbst zur Vorlage der entsprechenden Einkommenssteuerbescheide aufgefordert hätte.
Besonders gravierend war im vorliegenden Fall, dass die ARGE meinte, das Amtshilfeersuchen damit begründen zu müssen, dass bei dem Petenten der Verdacht des Sozialleistungsbetruges bestehe.

Ich habe die ARGE aufgefordert, in zukünftigen Fällen vor Anfragen bei anderen Behörden sorgfältiger zu prüfen, ob entsprechend dem datenschutzrechtlichen Grundsatz des Vorranges der Datenerhebung beim Betroffenen, der Betroffene selbst zur Klärung von Sachverhalten beitragen kann.

10.6 Beauftragung externer Gutachter im Schwerbehindertenverfahren

Ein Petent hat sich mit folgender Beschwerde an meine Dienststelle gewandt:
Der Petent hatte beim Landesamt für Jugend, Soziales und Versorgung einen Antrag auf Anerkennung einer Schwerbehinderung gestellt. Im Rahmen des Feststellungsverfahrens wurde seine Akte mit sämtlichen medizinischen Patientenunterlagen einem sogenannten „externen Gutachter“ zur Beurteilung vorgelegt. Ein externer Gutachter ist ein Arzt, der nicht beim Landesamt für Jugend, Soziales und Versorgung beschäftigt ist; das Landesamt bedient sich dieser Gutachter, wenn unter anderem deren besondere Fachkunde gefragt ist.

Im vorliegenden Fall war der Petent selbst Arzt und der beauftragte Gutachter ein Kollege des Petenten.
Der Petent war verständlicherweise entsetzt, dass sensible medizinische Informationen auf diesem Weg einem Arbeitskollegen zur Kenntnis gelangt waren. Er meint, es müsse für ihn als Patienten klar erkennbar sein, an welche Stellen oder Personen seine Patientenunterlagen weitergeleitet werden und dies im Voraus, so dass er die Möglichkeit habe, gegebenenfalls dagegen einzuschreiten.

Das Landesamt hat eingeräumt, dass aus dem Antragsformular nicht erkennbar sei, dass die Schwerbehindertenunterlagen externen Gutachtern zur Beurteilung vorgelegt werden. Es wurde zugesagt, in einer Neuauflage einen entsprechenden Hinweis aufzunehmen.

Nicht folgen will das Landesamt allerdings meinem Vorschlag, dem Antragsteller den konkret ausgewählten Gutachter mit der Möglichkeit eines Widerspruchsrechts zu benennen. Das Landesamt hat hierzu mitgeteilt, dass der Name des Gutachters dem Antragsteller nur in den Fällen mitgeteilt werde, in denen eine körperliche Untersuchung erforderlich sei. In diesen Fällen müsse das Vertrauensverhältnis zwischen Antragsteller und Arzt gewahrt sein, um aussagefähige und objektive Gutachten zu erhalten. Ebenso seien praktische Erwägungen, wie z.B. der Anfahrtsweg, zu berücksichtigen.

Anders seien dagegen ärztliche Stellungnahmen nach Aktenlage zu beurteilen. Von Rechts wegen sei die namentliche Benennung des ausgewählten Gutachters nicht geboten. Nach der maßgeblichen Vorschrift des § 76 SGB X sei der Betroffene nur in allgemeiner Form auf sein Widerspruchsrecht hinzuweisen. Bei jährlich etwa zwanzigtausend ärztlichen Stellungnahmen durch Außengutachter sei der erforderliche Aufwand bei vorheriger Unterrichtung der Antragsteller unverhältnismäßig. Außerdem würden die Bearbeitungsfristen durch eine solche Verfahrensweise unzumutbar verlängert.

Ich musste dem Landesamt für Jugend, Soziales und Versorgung darin recht geben, dass eine zwingende rechtliche Notwendigkeit, den Antragsteller vor Beauftragung eines externen Gutachters darüber zu informieren, wer der jeweilige Gutachter in

seinem Verfahren ist, nicht existiert. Ich habe auch Verständnis für die Argumentation des Landesamtes, dass es einen unverhältnismäßigen Aufwand bedeuten würde, bei der Vielzahl der ärztlichen Stellungnahmen die Betroffenen jeweils über den konkret ausgewählten Gutachter zu informieren, so dass ich im Ergebnis eine entsprechende Forderung nicht aufrecht erhalten habe.

10.7 Datenschutzprüfung bei einem kommunalen Träger

Mit dem 1.1.2005 wurden die Arbeitslosenhilfe und die Sozialhilfe für erwerbsfähige Hilfebedürftige zusammengeführt. Dieser Personenkreis erhält nunmehr Leistungen nach dem Zweiten Buch des Sozialgesetzbuches. Zu diesen Leistungen gehören insbesondere die Unterstützung erwerbsfähiger Hilfebedürftiger mit dem Ziel der Eingliederung in Arbeit sowie Leistungen zur Sicherung des Lebensunterhalts einschließlich der angemessenen Kosten für Unterkunft und Heizung in Form des Arbeitslosengeldes II. Wahrgenommen werden diese Aufgaben entweder von den sogenannten ARGE'n, das sind Zusammenschlüsse der Bundesagentur für Arbeit und den kreisfreien Städten oder Kreisen oder den zugelassenen kommunalen Trägern. Ein solcher zugelassener kommunaler Träger ist der Landkreis St. Wendel.
Es liegt auf der Hand, dass sowohl für eine Arbeitsvermittlung als auch für die Berechnung des Arbeitslosengeldes II eine Vielzahl sensibler Sozialdaten verarbeitet werden müssen, was für mich der Anlass war, bei einem Leistungsträger die Einhaltung der datenschutzrechtlichen Regelungen zu überprüfen.

Die Prüfung bei der Kommunalen Arbeitsförderung des Landkreises St. Wendel erstreckte sich auf die Einhaltung technisch-organisatorischer Datenschutzstandards sowie auf spezielle Fragestellungen im Zusammenhang mit der Aufgabenwahrnehmung nach dem SGB II.

Als Ergebnis meiner Prüfung kann ich feststellen, dass es sowohl Anlass zu Lob als auch zu Kritik gegeben hat.
Vorbildlich ist die Raumsicherung im Gebäude der Kommunalen Arbeitsförderung unter datenschutzrechtlichen Aspekten gelöst.

Durch die Konzentration des Publikumsverkehrs auf die untere Etage ist praktisch ausgeschlossen, dass sich ein Unbefugter Zutritt zu den Räumen der oberen Etage verschafft. Sollte sich dennoch jemand in der oberen Etage, in der die Leistungsabteilung untergebracht ist, Zugang verschaffen wollen, so sind zusätzliche Absperrmaßnahmen wie eine Sicherheitstür zur oberen Etage und die Türen der jeweiligen Sachbearbeiter zu überwinden, die jeweils nur mittels Transponder, die an jeden Mitarbeiter der Kommunalen Arbeitsförderung ausgegeben wurden, geöffnet werden können.
Die Kunden werden über ein Aufrufsystem, also ohne eine Namensnennung, in die Büros der Sachbearbeiter gebeten. Alle Büros im Gebäude sind Einzelbüros, wodurch ein Mithören schutzwürdiger Daten in den Sachbearbeitungsräumlichkeiten durch Dritte ausgeschlossen ist.
Eine Verbesserung habe ich allerdings angeregt:
So sollte durch eine Markierung vor der Informationstheke, an der sich jeder Kunde zunächst anmelden muss, deutlich gemacht werden, dass eine Diskretionsabstand eingehalten wird.

In folgenden Punkten habe ich Defizite feststellen müssen:

- Eine Risikoanalyse und ein IT-Sicherheitskonzept, mit deren Hilfe geeignete technische und organisatorische Maßnahmen getroffen werden können, um die Datensicherheit und den Datenschutz im erforderlichen Maße sicherzustellen, waren nicht vorhanden (bei der Prüfung konnte allerdings festgestellt werden, dass die technischen Lösungen auf schon sehr hohem Stand sind und insofern das Sicherheitskonzept die Notwendigkeit der getroffenen Maßnahmen nur weitgehend bestätigen wird).
- Ein Notfallkonzept war nicht vorhanden. Ein solches sollte erstellt und aufgrund der Ergebnisse der Notfallübungen fortgeschrieben werden.
- Protokolldateien zur Zugriffsprotokollierung werden zwar erstellt, aber nicht ausgewertet. Die Protokolldateien sollten im Rahmen einer IT-Revision regelmäßig überprüft und gelöscht werden.
- Für die Leistungsberechnung sowie die Eingliederung in Arbeit ist ein Programm im Einsatz, für das weder die vorgeschriebene Vorabkontrolle durchgeführt noch eine Verfahrensbeschreibung erstellt wurde. Auch ist vor der Freigabeentscheidung meine Dienststelle, nicht wie gesetzlich vorgesehen, beteiligt worden.

- Bemängelt habe ich die Art und Weise der Vernichtung der täglich anfallenden Papierabfälle mit personenbezogenen Daten. Diese werden von den Mitarbeiterinnen der Reinigungsfirma eingesammelt und zu dem bereitgestellten Datenschutzcontainer gebracht. Den Einwand der Kommunalen Arbeitsförderung, dass eine Entsorgung des anfallenden Papiers durch die einzelnen Bediensteten wegen der großen Menge nicht sachgerecht sei, habe ich nicht gelten lassen. Selbst wenn im Einzelfall größere Mengen von zu entsorgendem Schriftgut mit personenbezogenen Daten anfallen, scheint es mir im Hinblick auf die Sensibilität dieser Daten verhältnismäßig, wenn die Mitarbeiter sich in gewissen Zeitabständen zu dem Abfallcontainer begeben und die Unterlagen dort einwerfen.
- Der Landkreis St. Wendel hat den stellvertretenden Leiter der Kämmerei mit den „Aufgaben der Koordinationsstelle Datenschutz (gleich behördlicher Datenschutzbeauftragter gemäß § 8 Absatz 1 SDSG)“ betraut.

  Gleichzeitig hat der Landkreis „von der Möglichkeit Gebrauch gemacht, dem Landesbeauftragten für Datenschutz die Führung der Verfahrensverzeichnisse (§ 8 Absatz 2 Ziffer 1 SDSG) und die Durchführung der Vorabkontrolle (§ 8 Absatz 2 Ziffer 2 SDSG) zu übertragen.“

  Eine solche Rechtskonstruktion sieht das Saarländische Datenschutzgesetz nicht vor. Wenn ein behördlicher Datenschutzbeauftragter bestellt ist (§ 8 Absatz 1 SDSG) hat er die ihm gesetzlich zugewiesenen Aufgaben wahrzunehmen. Hierzu gehören insbesondere die Führung der Verfahrensbeschreibungen sowie die Durchführung der Vorabkontrolle (§ 8 Absatz 2 SDSG).

Über diese technisch-organisatorischen Datenschutzmängel hinaus habe ich folgende SGB II-spezifische Problemfelder angesprochen:

- Beim ersten Kontakt mit dem Arbeitsvermittler muss ein Formular ausgefüllt werden, in dem neben den persönlichen Daten wie Name, Adresse, Geburtsdatum, Familienstand usw. Angaben zur familiären und wirtschaftlichen Situation, zu betreuenden Kindern, zur beruflichen Qualifikation, zur Mobilität, zu Bewerbungsaktivitäten und gesundheitlichen Einschränkungen erhoben werden.

  Datenschutzrechtliche Bedenken habe ich hinsichtlich der Frage nach Vorstrafen sowie nach dem Bestehen gesundheitlicher Einschränkungen erhoben. Die undifferenzierte Frage nach Vorstrafen halte ich für unzulässig. Die Zulässigkeit der Daten, die im Rahmen der Arbeitsvermittlung erhoben werden, hat sich danach

zu richten, ob sie für einzugehende Beschäftigungsverhältnisse erforderlich sind. Nach der ständigen Rechtssprechung des Bundesarbeitsgerichts darf der Arbeitgeber den Bewerber bei der Einstellung nur nach Vorstrafen fragen, wenn und sowie die Art des zu besetzenden Arbeitsplatzes dies erfordert. Insofern scheidet die allgemeine Frage nach Vorstrafen, wie sie in dem Dokumentationsbogen vorgesehen war, aus. Die Kommunale Arbeitsförderung St. Wendel hat meinen Einwand aufgegriffen und fragt künftig nur noch bedarfsorientiert im Falle der Vermittlung in eine hiervon berührte Arbeit oder Arbeitsgelegenheit (z.B. Frage nach Verkehrsstraftaten bei der Vermittlung in eine Arbeit als Fernfahrer). Bei der Frage nach gesundheitlichen Einschränkungen darf meiner Auffassung nach nicht nach der Art der gesundheitlichen Einschränkung gefragt werden, sondern nur danach, ob eine Hilfebedürftiger bestimmte Tätigkeiten mit bestimmten Belastungen (z.B. häufiges Bücken, Heben von Gewichten, Schichtarbeit) leisten kann.

Die gleiche Problematik stellt sich bei dem Formular „Sozialmedizinische Leistungsbeurteilung“, das von dem Gesundheitsamt bei einem amtsärztlichen Gutachten verwandt wird. Auch hier ist nicht erkennbar, aus welchem Grund dem Sachbearbeiter im Vermittlungsbereich die Art der Erkrankung des Hilfebedürftigen mitgeteilt werden muss. Hier ist es ausreichend, wenn vom Gesundheitsamt mitgeteilt wird, welche Art von Tätigkeiten sowie in welchem Umfang der Hilfebedürftige ausüben kann.

- Erwerbsfähige Hilfsbedürftige, die aus medizinischen Gründen eine kostenaufwändige Ernährung brauchen, erhalten hierzu einen Mehrbedarf in angemessener Höhe (§ 21 Absatz 5 SGB II). Der Nachweis für die Notwendigkeit einer kostenaufwändigen Ernährung wird durch eine Bescheinigung des behandelnden Arztes erbracht, in dem die genaue Art der Erkrankung, wie z.B. HIV-Infektion, Krebserkrankung, Multiple Sklerose, und die daraus resultierende Kostform angegeben werden müssen.

  Ich halte es nicht für notwendig, dass dem Sachbearbeiter die genaue Diagnose bekannt gegeben wird. Eine Lösung könnte darin bestehen, dass verschiedene Erkrankungen, die die gleiche Kostform erforderlich machen, unter einer Ziffer zusammengefasst werden. Die Bundesagentur für Arbeit hat für ihren Bereich den entsprechenden Vordruck in dieser Weise geändert, so dass es naheliegt, dass die Kommunale Arbeitsförderung St. Wendel entsprechend verfährt.

- Informiert habe ich mich über die Verfahrensweise bei der Vorlage von Kontoauszügen im Rahmen der Leistungsbewilligung.

  Dem Antragsteller obliegt bei der Beantragung von Sozialleistungen eine Mitwirkungspflicht. Gemäß § 60 Absatz 1 SGB I hat, wer Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Gesetzliche Vorgaben, ob und in welchem Umfang der Leistungsträger die Vorlage von Kontoauszügen verlangen darf, lassen sich der vorgenannten Vorschrift nicht entnehmen.

  Bei der Kommunalen Arbeitsförderung in St. Wendel wird die Vorlage der Kontoauszüge der letzten 3 Monate verlangt bei der erstmaligen Beantragung von Leistungen, bei einem Folgeantrag, bei Beantragung von einmaligen Beihilfen sowie bei Verdacht auf Vorliegen eines Missbrauchs von Sozialleistungen.

  Diese Vorgehensweise ist aus datenschutzrechtlicher Sicht akzeptabel.

  Die Kommunale Arbeitsförderung St. Wendel lässt Schwärzungen in Kontoauszügen bei Sollbuchungen zu, solange der zuständige Sachbearbeiter keinen Missbrauchsverdacht hat. Habenbuchungen dürfen dagegen nicht geschwärzt werden, weil grundsätzlich das gesamte Einkommen bei der Hilfegewährung zu berücksichtigen ist:

  In diesem Zusammenhang habe ich gefordert, dass die Antragsteller bei der erstmaligen Aufforderung zur Vorlage von Kontoauszügen darauf hingewiesen werden, dass und in welchem Umfang die Möglichkeit von Schwärzungen in den Kontoauszügen besteht.

  Was die Aufnahme der Kontoauszüge in die jeweilige Leistungsakte angeht, vertrete ich folgende Auffassung: Die Aufnahme der Kontoauszüge in die Akte würde eine Speicherung von Daten bedeuten, die nur zulässig ist, soweit dies für die Aufgabenerfüllung erforderlich ist (§ 67 c Absatz 1 SGB X). Demnach dürfen Kontoauszüge nur dann in die Akte aufgenommen werden, wenn ein Verdacht auf Missbrauch vorliegt oder die Behörde aufgrund von Unstimmigkeiten in den vorgelegten Kontoauszügen weitergehende Maßnahmen ergreift. Ansonsten ist ein bloßer Vermerk des zuständigen Sachbearbeiters in der jeweiligen Akte ausreichend, um die Richtigkeit der Angaben des Antragstellers aufgrund der vorgelegten Kontoauszüge zu dokumentieren. An diese Vorgaben hält sich die Kommunale Arbeitsförderung St. Wendel.

11 Gesundheit

11.1 Die Elektronische Gesundheitskarte

Viele werden sich fragen, was aus der elektronischen Gesundheitskarte, von der immer wieder berichtet wird, mittlerweile geworden ist. Ich möchte deshalb an dieser Stelle über den Sachstand berichten.

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

Bereits in meinem letzten Tätigkeitsbericht (20. Tätigkeitsbericht 2003/2004, Teilziffer 9.4) habe ich die gesetzgeberischen Vorgaben zur Ausgestaltung und Verwendung der elektronischen Gesundheitskarte als in hohem Maße datenschutzfreundlich bezeichnet und darauf hingewiesen, dass es darauf ankommt, diese Vorgaben auch in die Praxis umzusetzen.

Der Termin 1. Januar 2006 zur Einführung der elektronischen Gesundheitskarte ist mittlerweile verstrichen, was damit zu erklären ist, dass es sich hier um das größte IT-Projekt in Deutschland handelt. Betroffen sind 80 Millionen Versicherte, 260 Krankenversicherungen, 2 200 Krankenhäuser, 21 000 Apotheken und 188 000 Ärzte.

Am 11. Oktober 2006 ist die „Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte“ in Kraft getreten. Ausgehend von dieser Verordnung haben inzwischen in mehreren Testregionen Feldtests mit jeweils 10 000 Versicherten begonnen. Das Saarland ist keine Testregion.

Die jeweils zuständigen Datenschutzbeauftragten sind in die Durchführung der Projekte einbezogen und achten darauf, dass den gesetzlichen Vorgaben entsprochen wird.

Da die Verarbeitung von Patientendaten im medizinischen Teil der Karte nur mit ausdrücklicher Einwilligung der Versicherten zulässig ist, müssen datenschutzgerechte Einwilligungserklärungen erarbeitet werden.

Die Versicherten haben das Recht, auf die auf ihrer Karte gespeicherten medizinischen Daten zuzugreifen. Wie dies in der Praxis funktioniert, ist Gegenstand der entsprechenden Testmaßnahmen.
Es muss darauf geachtet werden, dass der Versichertenstatus (einschließlich Status eines Sozialhilfeempfängers oder Teilnehmer eines Disease-Management-Programmes) verschlüsselt wird und nicht nach außen hin erkennbar ist.

Die 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Tagung am 10./11. März 2005 eine Entschließung zur Einführung der elektronischen Gesundheitskarte gefasst (Anlage 17.4) und darin insbesondere hervorgehoben, dass vorgesehene Einführungstermine kein Anlass dafür sein dürfen, von den bestehenden Datenschutzanforderungen Abstriche zu machen.

11.2 Gesetz zum Schutz von Kindern vor Vernachlässigung, Missbrauch, und Misshandlung

Im Berichtszeitraum haben mehrere Fälle schwerer Kindesmisshandlungen bundesweit Entsetzen ausgelöst. Diese Vorkommnisse haben eine leidenschaftliche Debatte darüber ausgelöst, mit welchen Mitteln solche Vorfälle in Zukunft vermieden werden können. Das Spektrum der Vorschläge reichte von einer verbesserten Aufklärung der Eltern und dem einfacheren Zugang zu Hilfsangeboten bis hin zu staatlichen Eingriffsmaßnahmen.
In die Diskussion eingebracht wurde die Idee, die gesundheitlichen Vorsorgeuntersuchungen im Kindesalter (U1 bis U9) für alle Eltern zur Pflicht zu machen. Nachdem eine entsprechende Bundesratsinitiative des Saarlandes gescheitert war, brachte die saarländische Landesregierung einen Gesetzentwurf ein, mit dem dieses Vorhaben zumindest in seinen Auswirkungen im Saarland umgesetzt werden sollte.
Zukünftig sollen alle Kinderärzte, die Früherkennungsuntersuchungen bei Kindern im Alter bis zu 5 ½ Jahren durchführen, einer Zentralen Stelle die Daten der Kinder und deren Eltern, die nicht an den Früherkennungsuntersuchungen teilgenommen haben, melden.
Die Meldebehörden übermitteln der Zentralen Stelle regelmäßig die erforderlichen Daten. Die Zentrale Stelle gleicht die Daten miteinander ab. Sie erinnert die Eltern

zunächst an die Teilnahme und meldet dann die Kinder, die immer noch nicht an der jeweiligen Vorsorgeuntersuchung teilgenommen haben, an das zuständige Gesundheitsamt. Das Gesundheitsamt nimmt Kontakt zu den Eltern auf und bittet diese um eine Vorstellung des Kindes bei einem niedergelassenen Arzt. Kommt es nicht zu einer Rückmeldung über die durchgeführte Untersuchung, übermittelt das Gesundheitsamt diese Tatsache an das zuständige Jugendamt, welches dann die weiteren erforderlichen Maßnahmen trifft.

In meiner Stellungnahme zu dem Gesetzentwurf habe ich herausgestellt, dass die vorgesehenen Maßnahmen in das Recht der Kinder und deren Erziehungsberechtigten auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes, sowie Artikel 2 der Saarländischen Verfassung eingreifen. Dieser Eingriff ist auch erheblich, denn wenn man den Kontext betrachtet, in dem die Daten gespeichert werden, so sind alle Eltern, die die Früherkennungsuntersuchungen ihrer Kinder nicht wahrgenommen haben, zunächst dem Generalverdacht ausgesetzt, ihre Kinder zu vernachlässigen, zu missbrauchen oder zu misshandeln. Ich habe auch auf die Gefahr hingewiesen, dass bei der Zentralen Stelle bzw. dem Gesundheitsamt eine Datei entsteht, in der alle Kinder bis zum Alter von 5 ½ Jahren gespeichert werden, die chronisch krank sind oder an einer Behinderung leiden. Denn diese Kinder brauchen an den Früherkennungsuntersuchungen nicht teilzunehmen, was bedingt, dass die entsprechenden Informationen der Zentralen Stelle bzw. dem Gesundheitsamt bekannt werden müssen.

Im Ergebnis habe ich allerdings deutlich gemacht, dass ich es als Landesbeauftragter für Datenschutz und Informationsfreiheit nicht als meine Aufgabe ansehe, die letztlich aus fachlicher Sicht zu entscheidende Frage zu beantworten, ob die geplanten Maßnahmen geeignet und erforderlich sind, einen Beitrag zum Schutz von Kindern vor Vernachlässigung, Missbrauch und Misshandlung zu leisten.
Gleichwohl habe ich an einigen Detailregelungen des Gesetzentwurfs Kritik geübt.
So ließ es der Gesetzentwurf völlig offen, welche Stelle die Aufgabe der Zentralen Stelle wahrnehmen soll. Ich bin der Auffassung, dass es sowohl das verfassungsrechtliche Gebot des Vorbehaltes des Gesetzes als auch die erforderliche Transparenz für die von der Datenspeicherung Betroffenen erfordert, diese Festlegung im Gesetz selbst zu treffen. Dieser Argumentation ist der Gesetzgeber letztlich gefolgt,

in dem er in dem Gesetz nunmehr die Aufgaben der Zentralen Stelle dem Universitätsklinikum des Saarlandes in Homburg übertragen hat.
Nicht aufgegriffen wurde dagegen mein Vorschlag, in das Gesetz eine Regelung aufzunehmen, wonach die Speicherung von Diagnosen und Befunden bei der Zentralen Stelle oder dem Gesundheitsamt nicht zulässig sind. Ich gehe aber zugunsten der Betroffenen davon aus, dass auch ohne einen ausdrücklichen Gesetzesbefehl diese Daten nicht gespeichert werden.

11.3 Mammographie-Screening

Mit einem parteiübergreifenden Bundestagsbeschluss vom 28. Juni 2002 wurde die Einführung eines qualitätsgesicherten, bundesweiten und bevölkerungsbezogenen Mammographie-Screening-Programms für Frauen zwischen 50 und 69 Jahren beschlossen. Ziel ist es, die Qualität gegenüber den herkömmlichen Brustkrebsvorsorgeuntersuchungen durch besondere Anforderungen an die fachliche Qualifikation der befindenden Ärzte sowie die Qualität der apparativen Ausstattung zu verbessern; Teambesprechungen der beteiligten Ärzte und radiologischen Fachkräfte sowie die Durchführung von Fallkonferenzen, wo der Behandlungsverlauf besprochen wird bzw. weitergehende therapeutische Maßnahmen nach Diagnosestellung empfohlen werden, sind ein weiterer Baustein.

Es liegt auf der Hand, dass im Rahmen der Durchführung dieses Programms in großem Umfang sensible medizinische Daten der teilnehmenden Frauen verarbeitet werden. Die Datenschutzbeauftragten des Bundes und der Länder sind deshalb von Anfang an von dem mit der Installation des Programms beauftragten Bundesausschuss der Ärzte und Krankenkassen beteiligt worden.
Mit Beschluss vom 15.12.2003 hat der Bundesausschuss der Ärzte und Krankenkassen in den „Krebsfrüherkennungs-Richtlinien“ den genauen Ablauf des Mammographie-Screenings von der Einladung der anspruchsberechtigten Frauen bis zu den Maßnahmen der Evaluation im Einzelnen geregelt.
Insbesondere zwei der in den Krebsfrüherkennungsrichtlinien vorgesehenen Maßnahmen machten nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder ein Handeln der jeweiligen Landesgesetzgeber erforderlich:

- Ein Problem betraf die ganz am Anfang des Programms stehende Einladung der betroffenen Frauen. In den Richtlinien ist hierzu vorgesehen, dass die Meldeämter zu diesem Zweck an eine Zentrale Stelle Vornamen, Familienname, frühere Familiennamen einschließlich Geburtsname, Geburtsdatum, Geburtsort und Anschrift übermitteln. Die Saarländische Meldedatenübermittlungsverordnung, die eine solche Datenübermittlung bisher nicht vorsah, wurde entsprechend geändert. Probleme bereitete die Frage, welche Stelle innerhalb des Landes die Aufgaben der Zentralen Stelle wahrnehmen sollte. Schnell wurde deutlich, dass man aus verfassungsrechtlichen Gründen diese Aufgabe nicht einfach durch Organisationsverfügung oder vertragliche Vereinbarung einer bestimmten Behörde übertragen kann. Die Lösung wurde schließlich dahingehend gefunden, dass nunmehr im Saarländischen Krebsregistergesetz geregelt ist, dass die Zentrale Stelle beim Ministerium für Justiz, Gesundheit und Soziales eingerichtet wird.

- In den Krebsfrüherkennungs-Richtlinien ist eine Verpflichtung zur Evaluation des Früherkennungsprogramms vorgesehen. So sollen z.B. Erkenntnisse darüber gewonnen werden, in wie vielen Fällen im Rahmen eines Mammographie-Screenings eine Krebserkrankung nicht erkannt worden ist (sogenannte falsch-negative Diagnosen). Die Richtlinien sehen hierzu einen Abgleich mit den Daten des jeweiligen Landeskrebsregisters vor. Auch in diesem Punkt musste das Saarländische Krebsregistergesetz geändert werden, da nach den bisher geltenden Bestimmungen des Krebsregistergesetzes ein solcher Abgleich nicht zulässig gewesen wäre.

Ich habe es in meiner Stellungnahme zu dem Gesetzentwurf begrüßt, dass durch die vorgesehenen Änderungen des Krebsregistergesetzes die von den Datenschutzbeauftragten des Bundes und der Länder betonte Notwendigkeit der Änderung landesgesetzlicher Vorschriften vor Aufbau des Mammographie-Screenings anerkannt wurde.
Im Saarland wurde mittlerweile mit der Durchführung des Mammographie-Screenings begonnen. Für den anstehenden Berichtszeitraum habe ich mir vorgenommen zu prüfen, ob die Verfahrensweise datenschutzrechtlich korrekt im Einklang mit den Vorschriften der Krebsfrüherkennungsrichtlinien erfolgt.

11.4 Abgleich der Daten der Besucher des Saarbrücker Drogenhilfezentrums mit dem Substitutionsregister der Kassenärztlichen Vereinigung

In Saarbrücken wurde Ende der 90-iger Jahre ein Drogenhilfezentrum eingerichtet. Neben der Beratung über Therapiemöglichkeiten, allgemeiner Sozialberatung, Gelegenheit zum Duschen und Essen, bietet das Drogenhilfezentrum Schwerstabhängigen die Möglichkeit, mitgebrachte Drogen unter hygienischen Bedingungen zu konsumieren.

Die Betreiber des Drogenhilfezentrums sind mit folgender Problematik an mich herangetreten:

Konsumenten, die sich in einer ärztlichen Substitutionsbehandlung befinden, seien von der Nutzung des Konsumraumes ausgeschlossen. Wesentlicher Hintergrund sei, dass für diese Konsumenten hohe medizinische Risiken bestehen, durch den unkontrollierbaren Mischkonsum Schaden zu erleiden; dieser Konsum könne zu lebensbedrohlichen Drogennotfällen im Drogenhilfezentrum führen.

Bisher könne allerdings im Drogenhilfezentrum nicht festgestellt werden, ob ein Substituierter dort Drogen konsumiere.

Um festzustellen, ob sich ein Konsument gleichzeitig in einer ärztlichen Substitutionsbehandlung befindet, hat das Drogenhilfezentrum vorgesehen, dass ein Mitarbeiter des Drogenhilfezentrums ein- bis zweimal im Monat die Einschreibeliste des Drogenhilfezentrums mit der Liste der bei der Kassenärztlichen Vereinigung gemeldeten Substituierten vergleicht.

Ich habe dem Dogenhilfezentrum mitgeteilt, dass ich diese Verfahrensweise datenschutzrechtlich wegen Fehlens einer Rechtsgrundlage, die die fragliche Datenübermittlung legitimieren könnte, nicht für zulässig halte.

Es wurde dann aber doch noch eine Lösung gefunden, die den berechtigten Anliegen des Drogenhilfezentrums Rechnung trägt. Der Abgleich soll mit codierten Listen stattfinden, so dass es nicht zu einer Übermittlung personenbezogener Daten kommt.

11.5 Bestellung eines Datenschutzbeauftragten bei der Psychotherapeutenkammer

Wie bereits in meinem 20. Tätigkeitsbericht erwähnt, ist aufgrund einer Änderung des Heilberufekammergesetzes die Psychotherapeutenkammer des Saarlandes errichtet worden. Diese hat sich an meine Dienststelle gewandt und um Auskunft gebeten, ob sie einen behördlichen Datenschutzbeauftragten bestellen muss oder ob meine Dienststelle diese Aufgabe wahrnimmt.

Gemäß § 8 des Saarländischen Datenschutzgesetzes können öffentliche Stellen, wozu auch die Psychotherapeutenkammer des Saarlandes zählt, einen behördlichen Datenschutzbeauftragten bestellen. Eine Verpflichtung für öffentliche Stellen im Saarland zur Bestellung eines Datenschutzbeauftragten besteht demnach nicht. Wird kein behördlicher Datenschutzbeauftragter bestellt, muss die Wahrnehmung von dessen Aufgaben durch die öffentliche Stelle selbst, mit Ausnahme der Führung des Verfahrensverzeichnisses nach § 9 SDSG und der Vorabkontrolle gemäß § 11 SDSG, sichergestellt werden. Das Verfahrensverzeichnis und die Vorabkontrolle werden in diesen Fällen von meiner Dienststelle übernommen. Näheres zur Vorabkontrolle und zum Verfahrensverzeichnis kann auch unserem Internetangebot unter www.lfdi.saarland.de entnommen werden.

11.6 Einsicht in die Patientenakten der Piloten bei dem flugmedizinischen Sachverständigen

Ein Arzt mit der Zulassung als flugmedizinischer Sachverständiger wandte sich hilfesuchend mit folgender Frage an meine Dienststelle:

Piloten müssen bestimmte gesundheitliche Anforderungen erfüllen, die durch ein Tauglichkeitszeugnis nachgewiesen werden. Diese Tauglichkeitsuntersuchungen werden von Ärzten durchgeführt, die hierzu eine besondere Zulassung benötigen. Die Zulassung muss alle drei Jahre durch die Luftaufsichtsbehörde beim Ministerium für Wirtschaft und Arbeit überprüft werden. Dabei hat die zuständige Stelle auch zu prüfen, ob die flugmedizinischen Tauglichkeitsuntersuchungen nach den geltenden Bestimmungen über die Anforderungen an die Tauglichkeit durchgeführt wurden.

Nachdem der betreffende Arzt einen Antrag auf Verlängerung seiner Zulassung gestellt hatte, besichtigten Mitarbeiter der Luftaufsicht seine Praxisräume und –ausstattung. Bei dieser Gelegenheit wollten sie auch Einsicht nehmen in die Patientenakten der Piloten. Dieses Ansinnen lehnte der Arzt unter Hinweis auf seine ärztliche Schweigepflicht ab. Er wollte von mir wissen, ob er sich richtig verhalten habe.

Zutreffend ist, dass die Pilotenakten beim flugmedizinischen Sachverständigen der ärztlichen Schweigepflicht gemäß § 203 StGB unterliegen. Ein Arzt, der unbefugt der ärztlichen Schweigepflicht unterliegende Tatsachen offenbart, macht sich strafbar.
Eine Befugnis zur Offenbarung kann sich insbesondere aus gesetzlichen Vorschriften ergeben. Das zuständige Ministerium hat sich auf § 24 e Absatz 7 der Luftverkehrs-Zulassungs-Ordnung berufen, wonach der flugmedizinische Sachverständige der zuständigen Stelle auf Verlangen die erforderlichen Auskünfte zu erteilen und die Einsicht in Dokumente zu gewähren hat.
Ob diese Vorschrift eine ausreichende Rechtsgrundlage darstellt, um in die Patientenakten der Piloten Einsicht zu nehmen, erscheint mir fraglich. Denn zum Einen handelt es sich bei der Luftverkehrs-Zulassungs-Ordnung um eine Verordnung. Ob die Verordnung in dem hier interessierenden Punkt eine ausreichende gesetzliche Grundlage hat, erscheint mir mehr als zweifelhaft. Außerdem ist der Vorschrift auch nicht mit der erforderlichen Deutlichkeit zu entnehmen, dass sich das Einsichtsrecht der Luftfahrtbehörde auch auf Patientenakten bezieht. Auch das zuständige Ministerium selbst äußerte schließlich Zweifel, ob es sich bei § 24 e Absatz 7 Luftverkehrs-Zulassungs-Ordnung um eine tragfähige Rechtsgrundlage handelt, um die ärztliche Schweigepflicht zu durchbrechen.
Beiden Rechtsgütern konnte schließlich dadurch Rechnung getragen werden, dass sich das Ministerium mit einer Einsichtnahme in geschwärzte Unterlagen, aus denen kein Rückschluss auf die Person des Untersuchten möglich ist, einverstanden erklärt hat.

11.7 Taschengeld im Maßregelvollzug

Ein Patient im Maßregelvollzug hat sich mit einer Eingabe an meine Dienststelle gewandt, weil er der Ansicht war, die Klinikleitung habe zu Unrecht die Angabe perso-

nenbezogener Daten von ihm verlangt. Maßregelvollzug ist die Unterbringung psychisch kranker Straftäter in einem psychiatrischen Krankenhaus (statt in einer Strafvollzugsanstalt).

Der Beschwerde lag folgender Sachverhalt zugrunde:

Der Petent hatte bei der Klinikleitung einen Antrag auf Gewährung von Taschengeld gestellt. In dem Antragsformular wurden auch Angaben über seine finanziellen Verhältnisse erhoben. Der Petent weigerte sich, diese Angaben zu machen und verwies auf die Vorschrift des § 22 Maßregelvollzugsgesetz (MRVG). Nach dieser Vorschrift erhält jeder Patient als Taschengeld einen angemessenen Barbetrag zur persönlichen Verfügung in entsprechender Anwendung der Vorschriften des Bundessozialhilfegesetzes. Nach Absatz 2 der Vorschrift kommt es bei der Gewährung von Taschengeld auf die Bedürftigkeit nicht an.

Auch ich habe aus dieser Vorschrift den Schluss gezogen, dass, wenn es auf die Bedürftigkeit nicht ankommt, auch keine Angaben über die Einkommens- und Vermögensverhältnisse erhoben werden dürfen.

In ihrer Stellungnahme teilte die Klinikleitung mit, dass es rechtens sein müsse, den Taschengeldanspruch von den Einkommens- und Vermögensverhältnissen abhängig zu machen, da nicht einsehbar sei, dass z.B. ein Renten- oder Pensionsempfänger zusätzlich ein Taschengeld von der Solidargemeinschaft erhalte. Im Falle des Petenten werde man ausnahmsweise auf die Erhebung der fraglichen Angaben verzichten.

Da mich diese Antwort nicht zufriedenstellte und ich selbst nicht nachvollziehen konnte, dass Patienten des Maßregelvollzugs Taschengeld erhalten sollen ohne Rücksicht auf ihre finanziellen Verhältnisse, habe ich die Fragestellung dem zuständigen Ministerium für Justiz, Gesundheit und Soziales vorgelegt. Die Antwort des Ministeriums brachte folgende Klärung: § 22 MRVG betreffe lediglich den Fall, dass der Patient einen bestimmten Teil seines Geldes als Taschengeld erhalten soll. Davon zu unterscheiden sei die Situation, dass ein Patient über kein eigenes Geld verfügt und sich ein Taschengeldanspruch dann nach den Vorschriften des Bundessozialhilfegesetzes ergebe. Dessen Regelungen sähen die Angabe der persönlichen Einkommens- und Vermögensverhältnisse zwingend vor.

§ 22 MRVG wurde wegen seiner missverständlichen Formulierung mittlerweile klarstellend im Sinne der Auffassung des Ministeriums geändert.

Das Ministerium hat versichert, dass zukünftig eine Nachfrage nach den Einkommens- und Vermögensverhältnissen nur noch in den Fällen erfolgt, in denen der Pa-

tient kein eigenes Geld zur Verfügung hat und zu seinen Gunsten ein Antrag an den Sozialhilfeträger zu stellen ist.

12 Schulen

12.1 Änderung des Schulordnungsgesetzes

Im Berichtszeitraum wurde das Schulordnungsgesetz geändert, das unter anderem die Rechtsverhältnisse zwischen Schule, Lehrer, Schüler und Erziehungsberechtigten regelt.
In das Gesetz aufgenommen wurden auch einige aus Datenschutzsicht bedeutsame Regelungen:
Als Reaktion auf den Amoklauf eines Schülers an einem Gymnasium in Erfurt im Jahre 2002 wurde eine Vorschrift geschaffen, die es der Schule unter bestimmten Voraussetzungen erlaubt, auch die Eltern bereits volljähriger Schüler über bestimmte Schulvorkommnisse zu unterrichten. Dies vor dem Hintergrund, dass man als eine mögliche Ursache für die Geschehnisse in Erfurt darin sieht, dass die Eltern des Amokschützen nichts davon wussten, dass ihr Sohn von der Schule verwiesen worden war.
Der Gesetzgeber hat nach meiner Auffassung einen ausgewogenen Ausgleich zwischen den Persönlichkeitsrechten des betroffenen Schülers und den Informationsinteressen seiner Eltern gefunden, indem eine Unterrichtung ohne Zustimmung nur bei fundamentalen schulischen Problemen, z.B. drohende Verfehlung des Klassenziels, Nichtteilnahme oder Nichtbestehen einer Abschlussprüfung, Ausschluss aus der Schule erfolgt. Außerdem ist der betroffene Schüler zu der beabsichtigten Unterrichtung anzuhören.

Bisher war es so, dass Schüler nicht verpflichtet waren, an Vergleichsuntersuchungen wie z.B. PISA teilzunehmen; die Teilnahme war vielmehr freiwillig und die Einholung des Einverständnisses der Erziehungsberechtigten erforderlich. Es ist für mich nachvollziehbar, wenn der Gesetzgeber die Teilnahme zur Pflicht macht, um eine lückenlose Beteiligung an diesen Untersuchungen zu gewährleisten.
Bei diesen Vergleichsuntersuchungen ist es allerdings ohne Belang, welcher einzelne bestimmte Schüler an einem Test teilgenommen hat. Eine Erhebung und weitere Verarbeitung personenbezogener Daten ist deshalb bei solchen Untersuchungen regelmäßig nicht erforderlich, wie die Erfahrungen gezeigt haben. Eine entsprechende Klarstellung wurde auf meine Anregung hin in das Gesetz aufgenommen.

Auf eines möchte ich an dieser Stelle hinweisen: Bei Vergleichsuntersuchungen geht es meist nicht nur um die Lösung von Testaufgaben in unterschiedlichen Bereichen, sondern meist sollen die Schüler und deren Erziehungsberechtigte Fragebogen ausfüllen. Das Ausfüllen dieser Fragebogen ist nach wie vor freiwillig und bedarf einer entsprechenden Einverständniserklärung der Beteiligten.

Neu aufgenommen wurde eine Vorschrift, wonach Bild- und Tonaufzeichnungen des Unterrichts zulässig sind, wenn die Betroffenen, bei minderjährigen Schülern auch die Erziehungsberechtigten, rechtzeitig über die beabsichtigte Aufzeichnung und deren Zweck in Kenntnis gesetzt worden sind und nicht widersprochen haben. Die Aufnahmen müssen dem Zweck der Lehrerbildung und der Fortentwicklung des Unterrichts dienen. Die Aufzeichnungen sind spätestens nach 5 Jahren zu löschen. Ich habe gefordert, dass die Daten schon früher gelöscht werden müssen, wenn schutzwürdige Belange des Betroffenen dies erfordern. Dieser Forderung wurde im Gesetz bedauerlicherweise nicht Rechnung getragen.

12.2 Änderung des Hochschulgebührengesetzes

Im Berichtszeitraum wurde das Saarländische Hochschulgebührengesetz geändert.
Während bisher eine Studiengebühr nur von den Studierenden erhoben wurde, die ihre Regelstudienzeit überzogen haben, erheben die Hochschulen ab dem Wintersemester 2007/2008 Studiengebühren von allen Studierenden.
Im Gesetzgebungsverfahren hatte ich Gelegenheit, zu dem Gesetzentwurf aus datenschutzrechtlicher Sicht Stellung zu nehmen.
Kritisch auseinandergesetzt habe ich mich mit der Vorschrift, die die Befreiung von der Studiengebühr vorsieht. Neben zwingenden Befreiungsgründen wie Kindererziehung, Schwerbehinderung, herausragenden sportlichen oder künstlerischen Leistungen, ist darüber hinaus eine fakultative Befreiung im Einzelfall vorgesehen.
Der Gesetzestext trifft keine Aussage dazu, unter welchen Voraussetzungen eine solche Befreiung im Einzelfall in Betracht kommt. Dies halte ich deshalb für problematisch, weil die Antragsteller sich zwangsläufig veranlasst sehen werden, umfangreiche Details aus ihrer persönlichen Lebenssituation preiszugeben, von denen sie zwar meinen, dass sie damit eine Befreiung erreichen können, auf die es für eine

Entscheidung über eine Befreiung möglicherweise aber überhaupt nicht ankommt. Es würde damit der das Datenschutzrecht beherrschende Grundsatz verletzt, dass eine öffentliche Stelle nur über die Informationen verfügen darf, die zu ihrer Aufgabenerfüllung unbedingt erforderlich sind. Ich habe deshalb eine Klarstellung im Gesetz gefordert, unter welchen Voraussetzungen eine Befreiung im Einzelfall möglich ist.
Dieser Forderung ist der Gesetzgeber nicht nachgekommen, hat aber die Hochschulen immerhin verpflichtet, in einer Gebührenordnung entsprechende Regelungen zu treffen.

12.3 Schülerstatistik

Im Berichtszeitraum sind Pläne der Kultusministerkonferenz bekannt geworden, die statistische Aufbereitung von Schülerdaten auf eine neue Grundlage zu stellen.
Diskutiert wurde, die Schullaufbahndaten eines jeden Schülers zur statistischen Auswertung auf Landesebene unter einer Identifikationsnummer zu speichern. Dabei soll jedes Land die gleichen Erhebungsmerkmale zugrunde legen (sogenannter Kerndatensatz).
In Rede stand darüber hinaus, dass die Länderdateien zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit sogenannten sozioökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist ebenfalls beabsichtigt.
Im Saarland ist es bisher so, dass die amtliche Schulstatistik über eine Erhebung von Summendatensätzen zu Schülerdaten vom statistischen Landesamt erstellt wird. Rechtsgrundlage ist das Schulordnungsgesetz (§ 20 d in Verbindung mit der „Verordnung über statistische Erhebungen an den Schulen und schulischen Einrichtungen sowie den Studien- und Landesseminaren im Saarland“ vom 31.8.2001). Auf die Frage des Ministeriums für Bildung, Kultur und Wissenschaft nach meiner Einschätzung der Zulässigkeit einer Erhebung von Schülerindividualdaten durch das Kultusministerium habe ich diesem mitgeteilt, dass ein solches Vorhaben auf jeden Fall eine Änderung der entsprechenden Rechtsvorschriften erforderlich machen würde. Deren Überprüfung auf Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit habe ich mir für das spätere Gesetzgebungsverfahren vorbehalten.

Länderübergreifend haben sich der Bundesbeauftragte und die Landesbeauftragten für Datenschutz auf ihrer Konferenz am 26./27. Oktober 2006 mit der Thematik befasst. In einer Entschließung (Anlage 17.22) haben sie dabei insbesondere die Notwendigkeit einer Totalerhebung in Frage gestellt, die nach den Vorgaben des Bundesverfassungsgerichtes nur zulässig ist, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf bereits vorliegende wissenschaftliche Untersuchungen (z.B. PISA, IGLU oder TIMSS) erscheine die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schülerbezogenen Bildungsregisters nicht dargetan.
Nachdrücklich fordern die Datenschutzbeauftragten den Verzicht auf eine Identifikationsnummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen müsse durch geeignete Verfahren ausgeschlossen werden.
Es müsse bei der gesamten Verfahrensgestaltung unbedingt darauf geachtet werden, dass das Statistikgeheimnis gewährleistet ist.

Positiv ist zu bewerten, dass die Kultusminister sich gegenüber Gesprächen mit den Datenschutzbeauftragten sehr offen gezeigt haben, so dass die begründete Erwartung besteht, dass ein Verfahren gefunden wird, das den Datenschutzbelangen ausreichend Rechnung trägt.

12.4 Schultests

Auch im letzten Berichtszeitraum gab es im Saarland eine Menge Schultests, an denen sich Schüler, Lehrer und Eltern beteiligen sollten. Angefangen vom bekanntesten Test PISA über KNULES, DEMAT, TIMSS, bis hin zu IGLU, mussten sich die saarländischen Lehrer und Schüler jede Menge Fragen stellen lassen. Grundlage für alle Erhebungen dieser Art ist § 20 e Absatz 1 Saarländisches Schulordnungsgesetz (SchoG), wonach Schüler und Lehrer dazu verpflichtet sind, an den von der Schulaufsichtsbehörde oder in deren Auftrag durchgeführten Vergleichsuntersuchungen sowie an sonstigen von der Schulaufsichtsbehörde vorgesehenen Maßnahmen zur Qualitätssicherung und zur Qualitätsentwicklung teilzunehmen. Darüber hinaus werden auch Fragen aus dem privaten und sozialen Umfeld der Schüler gestellt. Auskünfte aus diesem Umfeld sind jedoch nicht durch § 20 e Abs.1 SchoG abgedeckt

und dürfen nur auf freiwilliger Basis erhoben werden. Schüler unter 18 Jahren bedürfen dabei der Einwilligung ihrer Eltern. Vor der Erhebung der Daten müssen alle Beteiligten genau über den Verwendungszweck der Daten und über die Tatsache, dass bei Nichtbeteiligung keine Nachteile für Schüler und Eltern zu erwarten sind, aufgeklärt werden. Aus den in der Vergangenheit durchgeführten Schultests und den Genehmigungen durch die zuständige Schulaufsichtsbehörde nach Absprache mit meiner Dienststelle, hat sich eine Sensibilisierung der Schulaufsichtsbehörde zu den vorher angeführten Voraussetzungen ergeben. Auch in Zukunft wird das Miteinander von Schulaufsichtsbehörde und Datenschutz zentrales Thema vor der Genehmigung von weiteren Schultestes sein.

12.5 Bewertung von Hochschullehrern im Internet

Mehrere Professoren saarländischer Hochschulen haben sich bei meiner Dienststelle darüber beschwert, dass sie und ihre Lehrveranstaltungen im Internet von Studierenden bewertet werden.
Meine Recherchen haben ergeben, dass es eine Online-Plattform „meinprof.de“ für die Bewertung von Lehrveranstaltungen und Dozenten an deutschen Hochschulen gibt.
Studenten können hier ihre Professoren bewerten, in dem sie besuchte Veranstaltungen anhand von verschiedenen Kriterien und durch einen Freitextkommentar bewerten. Die Beurteilungen stehen jedermann zum Abruf über das Internet zur Verfügung.
Betrieben wird die Plattform von einem eingetragenen Verein mit Sitz in Berlin, so dass für die datenschutzrechtliche Kontrolle der Berliner Beauftragte für Datenschutz und Informationsfreiheit zuständig ist.

Manch einer wird der Auffassung sein, dass Professoren, die gewohnt sind, andere zu bewerten, es sich gefallen lassen müssen, auch mit Kritik konfrontiert zu werden. So einfach kann man es sich allerdings nicht machen; vielmehr muss sich die Datenverarbeitung nach den datenschutzrechtlichen Vorschriften richten, bei denen die Persönlichkeitsrechte der betroffenen Professoren angemessen berücksichtigt werden müssen. Gefahr für deren Persönlichkeitsrechte sehe ich unter verschiedenen

Gesichtspunkten: So steht dem Betroffenen keinerlei Möglichkeit zur Verfügung, auf den Inhalt seiner Bewertung Einfluss zu nehmen. Er muss Werturteile hinnehmen, die im Internet weltweit zur Verfügung stehen und von allen möglichen Interessierten gleich aus welchem Grund über Suchmaschinen abgerufen werden können. Auch ist nicht sichergestellt, dass die Bewertungen allein nach sachlichen Gesichtspunkten abgegeben werden; auch unlautere Motive wie Rachelust oder Schädigungsabsicht eines Konkurrenten, können zur Abgabe einer negativen Bewertung veranlassen. Der Vergleich mit einem modernen Pranger liegt nahe.

Nach massiver Kritik an ihrer Plattform bemühen sich die Betreiber um Verbesserungen. Um Missbrauch zu vermeiden, werden stichpunktartig die Neueintragungen überprüft. Rechtswidrige Äußerungen, wie z.B. Beleidigungen, werden aus der Datenbank entfernt. Den Dozenten wurde die Möglichkeit eingerichtet, zu den Bewertungen Stellung zu nehmen. Die Professoren können ihre Lehrveranstaltungen mit einem Passwort schützen, welches sie dann ihren Studierenden mitteilen können. Dadurch soll das Verfälschen der Ergebnisse durch Mehrfachbewertungen und Abgabe von Bewertungen durch Dritte, die eventuell gar nicht an der Veranstaltung teilgenommen haben, verhindert werden.

Zuletzt möchte ich noch den Hinweis geben, dass sich jeder bei Beschwerden und Anregungen an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden kann.

12.6 Private Zeugnisprogramme und PDA`s bei Lehrern

Ich habe die Eingabe eines Lehrers erhalten, der nachfragte, ob beim Einsatz eines privaten PDA`s mit privat besorgter Zeugniserstellungssoftware datenschutzrechtliche Vorgaben zu beachten wären.
In meiner Antwort an den Lehrer bezog ich mich auf das Schulordnungsgesetz (hier insb. § 20b SchoG), sowie die zugehörige Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen. Darüber hinaus sind die Bestimmungen des Saarländischen Datenschutzgesetzes (SDSG) zu beachten. So ist gemäß § 7 Absatz 2 Satz 2 SDSG das Ministerium für Bildung, Kul-

tur und Wissenschaft (MBKW) für die Freigabe solcher Verfahren zuständig. Das MBKW hat für den Grundschulbereich ein Zeugnisprogramm zur Verfügung gestellt, dessen datenschutzrechtliche Anforderungen mit meiner Dienststelle abgestimmt wurden. Wenn wie in diesem Fall beabsichtigt, ein anderes Zeugnisprogramm verwendet werden soll, so muss der Einsatz eines solchen Programms und auch der Einsatz des dazu benutzten PDA`s zuvor mit Echtdaten vom MBKW getestet und freigegeben werden. Vor der Freigabe ist meine Dienststelle zu beteiligen.
Der Einsatz des Programms fällt unter die Regelung des § 5a der Verordnung, nach dessen Absatz 2 die Datensicherungsmaßnahmen im Sinne von § 11 Absatz 1 und 3 SDSG ausreichend sein müssen. Nach meinem Kenntnisstand trifft dies für PDA derzeit nicht zu. Außerdem ist in Absatz 3 des § 5a der Verordnung der Umfang der zulässigen Daten festgelegt, der Zeugnisnoten nicht enthält. Bezüglich der Zeugnisnoten gibt es in Absatz 4 eine Regelung, die davon ausgeht, dass die Noten nur im Rahmen der Zeugniserstellung gespeichert werden dürfen und nach Durchführung der Aufgabe unverzüglich zu löschen sind. Eine Nutzung des PDA in dem beabsichtigten Sinn halte ich daher nicht für zulässig.

12.7 DSL-Zugang zum Verwaltungs-PC einer Schule

Wie in dem unter TZ 12.6 genannten Fall wurde ich von einer Lehrerin gebeten, die Zulässigkeit einer DSL-Verbindung, die über den Server der Stadt zum Verwaltungs-PC einer Schule hergestellt werden sollte, datenschutzrechtlich zu überprüfen. Da auch hier die unter TZ 12.6 genannten Rechtsvorschriften einschlägig sind, muss das MBKW eine Freigabe vor Benutzung der Verbindung aussprechen.
Derzeit steht einem solchen Einsatz die Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen entgegen. Gemäß § 5 Abs.1 Satz 3 Nr.1b) der Verordnung dürfen für Verwaltungszwecke in den Schulen eingesetzte automatische Datenverarbeitungsanlagen nicht mit anderen vernetzt sein.
Das Ministerium arbeitet schon seit längerem an einer Neufassung der Verordnung unter Berücksichtigung der aktuellen technischen Gegebenheiten und Entwicklungen. Nach momentaner Gesetzeslage ist die Verbindung über den Server der Stadt nicht zulässig.

12.8 Gewerbliche Erstellung von Schülerausweisen

Die Fotografeninnung Pfalz-Saarland hat sich mit einer Eingabe an meine Dienststelle gewandt und einen Verstoß gegen Datenschutzrecht an Schulen angezeigt. Schulen im Saarland und Rheinland-Pfalz werden von Unternehmen, die sich auf Schulfotos spezialisiert haben, Angebote unterbreitet, wonach für jeden Schüler neben der regulären Fotoaktion gleichzeitig und für die Schule kostenlos ein Schülerausweis mit Foto und persönlichen Daten im Scheckkartenformat angefertigt wird. Im Vorfeld werden dem Unternehmen Vorname, Nachname und Geburtstag des betroffenen Schülers durch die Schulleitung zum Zweck der Schülerausweiserstellung übermittelt. Ich konnte mich bei meiner Antwort an die Fotografeninnung Pfalz-Saar natürlich nur auf die meiner Aufsicht unterliegenden Schulen im Saarland beziehen. Es handelt sich bei der Auskunft der Schule an das Unternehmen um eine Datenübermittlung von Schülerdaten an eine private Einrichtung. Einschlägig ist hier § 8 Absatz 4 der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen im Saarland. Demnach ist in jedem Fall, d.h. auch bei Vorliegen der Einwilligung des Betroffenen (oder dessen Eltern bei Minderjährigkeit), die Weitergabe von personenbezogenen Daten zu gewerblichen Zwecken oder Werbezwecken jeglicher Art an Einzelpersonen oder private Einrichtungen unzulässig. Einem Privatunternehmen, das dem Zweck der Vermarktung von Schulfotos nachgeht, dürfen im Saarland keine Schülerdaten durch die Schulleitung zur Verfügung gestellt werden. Der Fotografeninnung Pfalz-Saarland, die mir keine konkreten Einzelfälle nennen wollte, genügte diese Mitteilung, um ihre Mitglieder über die Zulässigkeit der Fotoaktionen zu informieren. Das Kultusministerium sollte seine Schulleiter über die Regelung des § 8 Absatz 4 der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen im Saarland unterrichten.

12.9 Internetangebote von Schulen

Das World Wide Web (kurz www) bietet die Möglichkeit, sich weltweit zu präsentieren. Diese Möglichkeit möchten auch immer mehr Schulen im Saarland nutzen und eine eigene Homepage ins Internet stellen. So hatte ich auch im Berichtszeitraum wieder einigen Schulen bei der datenschutzgerechten Gestaltung der Schulhomepage behilflich sein können. Im Internetangebot meiner Dienststelle unter

www.lfdi.saarland.de gibt es einen eigenen Unterpunkt für Schulen, um sich dort über den datenschutzgerechten Umgang mit Schulhomepages zu informieren und zahlreiches Informationsmaterial zu diesem Thema herunterladen zu können. Dort findet sich unter anderem ein Merkblatt „Schulen ans Netz – mit Sicherheit“ oder auch Antworten auf häufig gestellte Fragen zur Nutzung des Internet an Schulen.

Sehr häufig tritt bei der Erstellung einer Homepage der Wille der Schule auf, auch Bilder und Namen von Schülern, Lehrern, Eltern oder sonstigen Personen ins Netz zu stellen. Eine gesetzliche Befugnisnorm, die außerhalb der ureigensten Aufgabenerfüllung der Schule liegt, gibt es jedoch nicht. Eher im Gegenteil beschreibt § 22 des Kunsturhebergesetzes, dass eine Verbreitung von Lichtbildern von Personen im Regelfall nur mit deren Einwilligung zulässig ist.

Klassenfotos von minderjährigen Kindern dürfen also nur mit Zustimmung der Eltern im Internet veröffentlicht werden. Sollten sich die Eltern der Kinder gegen eine Veröffentlichung im Internet ausgesprochen haben, so sind Name und Gesicht des betroffenen Kindes unkenntlich zu machen oder zu entfernen. Am besten wird bei der Erstellung einer Schulhomepage ganz auf Bilder und Namensnennung (mit Ausnahme der verantwortlichen Schulleitung) verzichtet.

Daten und Bilder im Internet können Personen ein Leben lang begleiten (es gibt Archive und Caches) und auch zu Ihrem Nachteil verwendet werden. Es gibt mittlerweile Firmen, die sich darauf spezialisiert haben, Persönlichkeitsprofile aus dem Internet zu erstellen und ggf. einem möglichen Arbeitgeber vor einem Einstellungsgespräch zur Verfügung zu stellen. Nicht alle Auskünfte, die man im Internet über eine Person finden kann, müssen für eine spätere Einstellung von Vorteil sein.

13 Öffentlicher Dienst

13.1 Elektronische Verwaltungsvorschriften Informationssystem Saarland (ELVIS)

Im Jahre 2004 hatte die saarländische Landesregierung eine Suchmaschine zum Auffinden der saarländischen Verwaltungsvorschriften installiert. Während diese Suchmaschine zunächst nur den Bediensteten der Landesverwaltung intern zur Verfügung stand, wurde im Hinblick auf die gute Resonanz beschlossen, ELVIS im Internet einer breiten Öffentlichkeit zugänglich zu machen.

Vor diesem Schritt sollte ich die datenschutzrechtliche Seite des Vorhabens beurteilen.

Was hat eine Suchmaschine zum Auffinden von Verwaltungsvorschriften mit Datenschutz zu tun? Das Problem bestand darin, dass bei jedem Treffer auch die jeweiligen Ansprechpartner, d.h. die Bediensteten, die die Verwaltungsvorschrift erstellt haben oder zumindest dazu nähere Auskünfte erteilen können, namentlich mit Telefonnummer genannt sind; auch ihre E-Mail-Adresse ist personalisiert, d.h. der Name des betreffenden Mitarbeiters ist Bestandteil dieser Adresse.

Ich habe deutlich gemacht, dass ich die namentliche Nennung der Ansprechpartner nicht für erforderlich halte, da sie datenschutzrechtlich unzulässig ist. Nach der für die Verarbeitung von Mitarbeiterdaten maßgeblichen Vorschrift des § 31 Saarländisches Datenschutzgesetz ist eine Verarbeitung von Beschäftigtendaten nur zulässig, wenn dies unter anderem zur Durchführung des Dienst- oder Arbeitsverhältnisses erforderlich ist. Ich habe darauf hingewiesen, dass es ausreicht, wenn lediglich die Telefonnummern der Ansprechpartner angegeben werden; die E-Mail-Adresse sollte bei Internet-Zugriffen durch eine allgemeine Ansprechstelle ersetzt werden. In dem anschließenden Schriftverkehr wurde darauf hingewiesen, dass die Angabe von Ansprechpartnern und Mailadressen auch bei öffentlichen Stellen im Internet zum Standard geworden sei; nur so könne letztlich auch von einer bürgeroffenen Verwaltung und von Kundenorientierung gesprochen werden. Außerdem würde die Zwischenschaltung einer „Postmaster-Mailadresse“ zu Schwierigkeiten und Verzögerungen in der Anwendung führen. Ich habe trotz dieser Einwände an meiner Auffassung festgehalten, dass eine namentliche Benennung der Ansprechpartner sowie die Angabe personenbezogener E-Mail-Adressen datenschutzrechtlich nicht zulässig seien.

Dies hat nichts mit bürokratischer Gesetzesanwendung zu tun, sondern ist bedingt durch die realen Gefahren des Internets. Man muss sich vor Augen halten, dass Informationen über Betroffene mit Hilfe von Suchmaschinen beliebig zusammengeführt und zu einem Persönlichkeitsprofil verdichtet werden können. Im Laufe der Zeit kommt es dazu, dass man durch seine Präsentation in unterschiedlichen Internet-Angeboten für jedermann zum gläsernen Bürger wird.
Ich trete deshalb vehement dafür ein, dass mit personenbezogenen Daten im Internet so zurückhaltend wie nur möglich umgegangen wird, dass im Ergebnis personenbezogene Daten nur dann veröffentlicht werden sollen, wenn eine Verwaltungsaufgabe ohne sie nicht oder zumindest nicht vollständig, nicht zeitgerecht oder nicht rechtmäßig erfüllbar ist.
Es lässt sich wohl kaum bestreiten, dass eine Kontaktaufnahme mit dem zuständigen Bearbeiter auch möglich ist, wenn statt des Namens und der Telefonnummer nur die Telefonnummer angegeben ist. Statt individueller E-Mail-Adressen der Ansprechpartner könnte ein Formular eingestellt werden, das „im Betreff“ gleich die Bezeichnung der betroffenen Verwaltungsvorschrift enthält und anschließend automatisch durch systeminterne Einstellungen an den zuständigen Ansprechpartner weitergeleitet wird.
Trotz meiner geäußerten Bedenken ist die Suchmaschine mittlerweile wie von Anfang an geplant mit den personenbezogenen Angaben im Internet in Betrieb gegangen.

13.2 Saarländisches Sicherheitsüberprüfungsgesetz (SSÜG)

Die „Allgemeine Verwaltungsvorschrift zum Saarländischen Sicherheitsüberprüfungsgesetz (AV SSÜG)“ enthält in der Anlage 7 einen „Hinweis zum Widerspruchsrecht nach § 28 Abs. 1 Saarländisches Datenschutzgesetz (SDSG) bezüglich der Kontrolle von Akten über die Sicherheitsüberprüfung durch die oder den Landesbeauftragte(n) für den Datenschutz (LfD)“ und zusätzlich eine vorgefertigte „Erklärung“ über den Widerspruch.

Obwohl bei der Sicherheitsüberprüfung hochsensible personenbezogene Daten verarbeitet werden, wurde der Landesbeauftragte für Datenschutz vor Erlass der AV SSÜG nicht beteiligt.

Zwar ist die zu überprüfende Person über ihr Widerspruchsrecht zu belehren und ihre Entscheidung aktenkundig zu machen, durch die aktuelle Fassung der AV SSÜG entsteht jedoch der Eindruck, dass alle Vordrucke vollständig auszufüllen und abzugeben sind, somit auch die Widerspruchserklärung. Aus meiner Sicht darf diese Entscheidung nicht zu einem bestimmten Zeitpunkt (Abgabe der Sicherheitserklärung) abverlangt werden. Aktenkundig ist der Widerspruch erst zu machen, wenn sich die betroffene Person zu einem von ihr selbst bestimmtem Zeitpunkt zu ihrem Widerspruchsrecht geäußert hat.

Das Ministerium für Inneres wurde gebeten, den Hinweis zum Widerspruchsrecht anhand gültiger Rechtsbestimmungen zu berichtigen und die „Erklärung“ in Einklang mit der gesetzlichen Bestimmung des § 25 SSÜG zu bringen.

13.3 Beihilfe

13.3.1 Vorlage des Einkommensteuerbescheides zur Prüfung der Beihilfeberechtigung

Die zentrale Beihilfestelle beim „Landesamt für Zentrale Dienste“ hat im Jahr 2006 zur Überprüfung der Beihilfeberechtigung von Ehegatten die Vorlage des Einkommensteuerbescheides 2005 gefordert. Eine solche Datenerhebung ist gemäß § 12 Abs.1 SDSG nur zulässig, soweit sie zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Gemäß § 4 Abs. 7 der saarländischen Beihilfeverordnung ist ein Ehegatte nur dann beihilfeberechtigt, wenn der Gesamtbetrag der Einkünfte (Ehegattenanteil) nach dem Einkommensteuergesetz im Kalenderjahr vor der Antragstellung den Betrag von 15339,00 € nicht überschreitet. Die Überprüfung der Beihilfeberechtigung der Ehegatten gehört also unter anderem zur Aufgabenerfüllung der Zentralen Beihilfestelle und die dazu erforderliche Datenerhebung ist nach § 4 Absatz 1 SDSG zulässig.

Von Seiten der Zentralen Beihilfestelle wurde folgender Textbaustein im Beihilfebescheid verwandt:

„Im Rahmen einer generellen Überprüfung aller gleich gelagerten Fälle werden Sie gebeten, binnen eines Monats eine Kopie des Einkommensteuerbescheides für das Jahr 2005 bzw. einen geeigneten Einkommensnachweis vorzulegen, falls eine Veranlagung beim Finanzamt nicht durchgeführt wurde."

Gleich mehrere Petenten haben sich daraufhin an meine Dienststelle gewandt und das Vorgehen der Beihilfestelle aus datenschutzrechtlicher Sicht kritisiert, weil durch die Offenlegung Ihres Einkommensteuerbescheides auch Daten des Hauptbeihilfeberechtigten, die nicht zur Aufgabenerfüllung der Zentralen Beihilfestelle benötigt werden, wie zum Beispiel Mieteinkünfte mitgeteilt werden müssen.

Auf die Intervention meiner Dienststelle hin, dass der Vermerk im Beihilfebescheid so zu formulieren sei, dass deutlich wird, mit welchen Unterlagen der Nachweispflicht Genüge getan werden kann, insbesondere der Hinweis, dass in dem Einkommensteuerbescheid die Angaben zum Einkommen des Hauptbeihilfeberechtigten geschwärzt werden können, wurde folgender neuer Textbaustein im Beihilfebescheid eingebaut:

„ Im Rahmen einer generellen Überprüfung aller gleich gelagerten Fälle werden Sie gebeten, binnen eines Monats einen geeigneten Einkommensnachweis für das Jahr 2005 vorzulegen. In Betracht kommt eine Kopie des Einkommensteuerbescheides oder eine Nichtveranlagungsbescheinigung des zuständigen Finanzamtes. Die für den Einkommensnachweises Ihres Ehegatten nicht relevanten Daten können geschwärzt werden."

So wurde dem Erforderlichkeitsgrundsatz im Datenschutz (§ 12 Absatz 1 SDSG) Rechnung getragen und nur die zur Aufgabenerfüllung notwendigen Daten vom Beihilfeberechtigten angefordert.

13.3.2 Einscannen von Beihilfebelegen

Im Rahmen der unter TZ 2.5 dieses Tätigkeitsberichtes genannten Einführung eines Dokumentenmanagementsystems bei der Zentralen Besoldungs- und Beihilfestelle des Saarlandes trat die Frage auf, welche Daten im Scannerverfahren der Beihilfestelle eingescannt werden dürfen. Ich vertrete hierzu, wie viele meiner Kollegen die Auffassung, dass ein Einscannen von Belegen, aus denen die Art der Erkrankung des Beihilfeberechtigten erkennbar ist, nicht zulässig ist. Nach § 108 f Absatz 2 Satz 2 Saarländisches Beamtengesetz sind Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, unverzüglich zurückzugeben, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. Dies ist Ausdruck für die Sensibilität der Beihilfebelege. Bewusst hat der Gesetzgeber hier eine strenge Auslegung des Rechtes des Betroffenen auf Selbstbestimmung über seine Gesundheitsdaten gewählt, damit diese sensiblen Daten nicht zweckentfremdet werden können. Der Grund, zu dem die Beihilfestelle Belege vom Beihilfeberechtigten benötigt, erschöpft sich in der Beihilfeerstattung. Sobald der Beihilfebescheid erteilt wird, ist eine weitere Aufbewahrung der Belege nicht mehr erforderlich und somit unzulässig, da aus den meisten Belegen die Art der Erkrankung anhand der Diagnose ersichtlich ist oder man auf die Art der Erkrankung schließen kann. Im Saarland werden die Belege zusammen mit dem Beihilfebescheid an den Beihilfeberechtigten zurückgesandt. Ein Abweichen von dieser Regelung im Zusammenhang mit automatisierten Belegen wäre hier aus datenschutzrechtlicher Sicht ein Rückschritt und nicht wünschenswert.

13.4 Einsicht in die Zeiterfassungsdaten der Mitarbeiter

Seit Einführung der gleitenden Arbeitszeit in immer mehr Behörden und Dienststellen des Landes und der damit regelmäßig verbundenen automatisierten Zeiterfassung erreichen mich immer wieder Anfragen zum zulässigen Umgang mit den dabei gespeicherten personenbezogenen Daten der Mitarbeiter.

Exemplarisch möchte ich zwei Fragestellungen darstellen, die im Berichtszeitraum an mich herangetragen worden sind:

Leserecht des Betriebsrates auf die Zeitkonten der Beschäftigten

Der Betriebsrat hat nach § 80 Absatz 1 Nr. 1 Betriebsverfassungsgesetz die Aufgabe, darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen eingehalten werden. Unbestritten ist, dass sich die Überwachungspflicht des Betriebsrates auch auf Arbeitnehmerschutzvorschriften zur Arbeitszeit erstreckt. Welche Informationen dem Betriebsrat in diesem Zusammenhang zustehen, ist in § 80 Absatz 2 Betriebsverfassungsgesetz geregelt. Der Arbeitgeber hat danach den Betriebsrat rechtzeitig und umfassend zu unterrichten. Dem Betriebsrat sind auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Aus der Bestimmung, dass die Informationen (nur) „auf Verlangen" bereitzustellen sind, ergibt sich, dass ein ständiger Lesezugriff auf die automatisiert gespeicherten Daten nicht dem Willen des Gesetzgebers entspricht. Mit dem Begriff „jederzeit" wird lediglich ausgedrückt, dass der Arbeitgeber den Zeitpunkt der Informationsgewährung nicht bestimmen kann, sondern dass der Betriebsrat die Unterlagen dann beanspruchen kann, wenn er sie nach seiner Einschätzung zur Wahrnehmung der Überwachungspflicht benötigt.

Dem Betriebsrat sind die erforderlichen Unterlagen zur Verfügung zu stellen, d.h. die Informationen, die für seine Überwachungsaufgabe unerlässlich sind. Dass diese Informationen auch personenbezogene Daten enthalten können, sehe ich aufgrund dieser Vorschrift als zulässig an. Vielfach wird die Einhaltung der Bestimmungen erst anhand der konkret von den einzelnen Arbeitnehmern geleisteten Arbeitszeiten beurteilt werden können.

Aus meiner Sicht bestehen demnach keine Bedenken, wenn dem Betriebsrat auf Verlangen die Einsichtnahme in die gespeicherten Daten und/oder in die Ausdrucke bei der Personalabteilung gestattet wird. Ein ständiges Zugriffsrecht des Betriebsrates auf die Daten halte ich dagegen nicht für zulässig.

Informationen des Fachvorgesetzten über den Gleitzeitsaldo bei Beantragung von ganztägigem Freizeitausgleich

Der Personalrat einer Landesbehörde hat mich darüber informiert, dass für die Beantragung von ganztägigem Freizeitausgleich ein neues Formular eingeführt worden ist, in das der aktuelle Gleitzeitstand einzutragen ist.

Da der Antrag vom Fachvorgesetzten abgezeichnet werden müsse, erhalte dieser Kenntnis von Zeiterfassungsdaten seiner Mitarbeiter, was nach Ansicht des Personalrates deshalb unzulässig sein soll, weil die Kontrolle der Einhaltung der Arbeitszeitregelung allein Aufgabe der zuständigen Personalsachbearbeiter sei.
Die Behördenleitung verteidigt die Einführung des neuen Formulars im Wesentlichen damit, dass Unterschreitungen der Sollarbeitszeit über die nach der Dienstvereinbarung zulässigen 15 Stunden unterbunden werden sollen. Außerdem liege die Genehmigung des eintägigen Zeitausgleiches für den Fall, dass das Gleitzeitkonto kein Guthaben von mindestens 8 Stunden aufweise, im pflichtgemäßen Ermessen des Fachvorgesetzten.

Bei meiner datenschutzrechtlichen Bewertung habe ich die Vorschrift des § 4 Absatz 1 Saarländisches Datenschutzgesetz (SDSG) zugrunde gelegt, wonach eine Erhebung personenbezogener Daten nur zulässig ist, wenn das SDSG oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Nach § 31 Absatz 1 SDSG, der die Zulässigkeit der Datenverarbeitung bei Dienst- und Arbeitsverhältnissen regelt, dürfen Daten von Beschäftigten nur verarbeitet werden, wenn dies unter anderem zur Durchführung personeller Maßnahmen erforderlich ist.
Die Angabe des aktuellen Standes des Arbeitszeitkontos wäre erforderlich, wenn die Inanspruchnahme des ganztägigen Zeitausgleiches von einem bestimmten Stand des Arbeitszeitkontos abhängig wäre. Die einschlägige Dienstvereinbarung über die Arbeitszeitregelung enthält hierzu keine eindeutige Aussage. Wenn es dort heißt: „Die Inanspruchnahme von Freizeitausgleich erfolgt unter Beachtung dienstlicher Belange in Abstimmung mit dem/der unmittelbaren Vorgesetzten“ so spricht dies eher dafür, dass der aktuelle Gleitzeitstand bei der Gewährung des Freizeitausgleiches keine Rolle spielt und es nur auf die dienstlichen Belange ankommt. Ich habe darauf hingewiesen, dass die Auslegung dieser Vorschrift zunächst zwischen den Beteiligten geklärt werden muss, weil davon die datenschutzrechtliche Bewertung der Erforderlichkeit abhängt.

Das Argument, dass es in der Vergangenheit Bedienstete gegeben habe, die ihr Arbeitszeitkonto in einer Größenordnung überzogen hatten, dass sie nicht mehr in der Lage waren, die Unterschreitungen durch Nacharbeit auszugleichen, hat mich ebenfalls nicht überzeugt. Ich räume zwar ein, dass die Angabe des Gleitzeitsaldos vor

Inanspruchnahme des eintägigen Freizeitausgleiches bei einigen „schwarzen Schafen“ ein geeignetes Mittel darstellt, diese Personen zur Einhaltung ihrer Dienstpflichten zu bringen. Gleichwohl halte ich es für unverhältnismäßig, dass wegen des dienstwidrigen Verhaltens einzelner Personen alle anderen rechtstreuen Mitarbeiter zur Offenbarung nicht erforderlicher Angaben gezwungen werden.
Bei Redaktionsschluss war nicht bekannt, welchen Abschluss die Angelegenheit gefunden hat.

Hinweisen möchte ich auf eine Musterdienstvereinbarung für die automatisierte Zeiterfassung, die unter meiner Internet-Adresse www.lfdi.saarland.de abgerufen werden kann.

13.5 Vorabkontrolle einer Personalverwaltungssoftware

Im November letzten Jahres, trat eine behördlich bestellte Datenschutzbeauftragte mit der Bitte an mich heran, sie bei Ihrem ersten Vorabkontrollverfahren gemäß § 11 Absatz 1 SDSG als Datenschutzbeauftragte zu unterstützen. Es handelte sich dabei um ein neues Personal- und Stellenverwaltungsmodul, das in der Behörde eingesetzt werden sollte. Durch das vorbildliche Zusammenspiel zwischen behördlicher Datenschutzbeauftragten und meiner Dienststelle konnten schon im Vorfeld der Einführung des Moduls grundlegende datenschutzrechtliche Eckpfeiler für die später erfolgte Zustimmung gesetzt werden. Strittige Punkte waren hierbei zum einen der zugriffsberechtigte Personenkreis und zum anderen die Erfassung des Grades der Behinderung. So sollte anfangs jedem Abteilungsleiter die Einsicht über Fehlzeiten und Krankheitstage aller Beschäftigten in der Behörde gewährt werden. Wir konnten die Zugriffsrechte der Abteilungsleiter auf die jeweilige Abteilung beschränken. Es ist zur Aufgabenerfüllung des Abteilungsleiters X nicht erforderlich, die Fehltage der Mitarbeiter des Abteilungsleiters Y einzusehen. Zur Eingabe des Grades der Behinderung wurde von meiner Seite aus vorgebracht, es sei entgegen der ursprünglichen Vorgabe nicht notwendig, den genauen Grad der Behinderung mitzuteilen. Da in § 125 SGB IX für den hierbei relevanten Zusatzurlaub von fünf Tagen lediglich die Eigenschaft als Schwerbehinderter ausschlaggebend ist, wurde das Programm derart ab-

geändert, dass man jetzt die Eingabe der Schwerbehinderteneigenschaft nur noch mit Ja oder Nein zu markieren hat. Auch hier hat sich einmal mehr gezeigt, wie positiv ein konstruktives Miteinander von Behörden und Datenschutz sein kann. Alle datenschutzrechtlichen Vorgaben meiner Dienststelle wurden bei der Umsetzung des Moduls frühzeitig berücksichtigt und das Programm dementsprechend angepasst.

13.6 Datenschutzprüfung bei Telearbeitsplätzen

Wie in meinem 20. Tätigkeitsbericht unter TZ 12.5 angekündigt, habe ich im letzten Berichtszeitraum die Einhaltung der „Richtlinie zur Einführung von Telearbeit in der Landesverwaltung“ überprüft. Dabei wurden zwei Telearbeitsplätze aus den Ressorts Ministerium für Finanzen und Ministerium für Inneres, Familie, Frauen und Sport vor Ort besichtigt. Die Vorgaben der Richtlinie zur Einführung von Telearbeit in der Landesverwaltung wurden bei beiden Telearbeitsplätzen größtenteils eingehalten. Es handelte sich jeweils um ein separates, abschließbares Arbeitszimmer in der Wohnung des Bediensteten. Die dort gelagerten personenbezogenen Daten wurden in abschließbaren Möbeln aufbewahrt. Der Transport der Akten von der Dienststelle zum Telearbeitsplatz und zurück erfolgte in einem Fall in einer Wäschewanne, die mittels eines Plastiksacks „verschlossen“ wird. Dies genügt nicht den Anforderungen des Datenschutzes und der Dienstherr wurde aufgefordert, ausreichend große abschließbare Behälter zur Verfügung zu stellen. Als weiterer Mangel wurde festgestellt, dass bei einem Telearbeitsplatz die Aktenvernichtung mittels eines privaten Aktenvernichters durchgeführt wurde, der nicht den Anforderungen der „Richtlinie des Ministeriums des Inneren zur Vernichtung von Schriftgut und sonstigen Datenträgern“ vom 09.01.1989 entspricht. Hier wurde gefordert, dass entweder von Seiten des Ministeriums ein entsprechender Aktenvernichter zur Verfügung gestellt werden muss oder die Akten im Ministerium selbst vernichtet werden sollen. Aus technischer Sicht war bei einem Telearbeitsplatz auf der Standardoberfläche des zur Verfügung gestellten PC über den Internet Explorer ein normaler Internetzugang möglich. Zwar sind die dienstlichen Zugänge auf dem Server beim Ministerium über einen VPN-Tunnel geschützt, doch besteht die Gefahr, dass über den Internetzugang unerkannt Schadsoftware auf dem PC lokal installiert wird, die dann beim VPN-Zugriff aktiv werden kann. Es wurde gefordert, den Internetzugang des Dienst-PC über den

VPN-Tunnel und das Landesdatennetz erfolgen zu lassen und die lokale Aktivierbarkeit des Internet-Explorers abzuschalten.

13.7 Wahlberechtigte zur Schwerbehindertenvertretung am „Schwarzen Brett“

Die Arbeitsgemeinschaft der Schwerbehindertenvertretungen des öffentlichen Dienstes im Saarland bat mich um Stellungnahme, ob es zulässig sei, eine Liste mit Wahlberechtigten zur Wahl des Schwerbehindertenvertreters öffentlich am „Schwarzen Brett“ der Dienststelle auszustellen.

Nach § 3 Abs.1 der Wahlordnung der Schwerbehindertenvertretung (SchwebVWO) muss der Wahlvorstand eine Liste der Wahlberechtigten aufstellen. In dieser Liste sollen die Wahlberechtigten mit Familienname, Vorname, erforderlichenfalls Geburtsdatum sowie Betrieb oder Dienststelle in alphabetischer Reihenfolge aufgeführt werden. Ist die Liste vollständig, muss sie unverzüglich nach Einleitung der Wahl bis zum Abschluss der Stimmabgabe an geeigneter Stelle zur Einsichtnahme ausgelegt werden (§ 3 Abs.2 SchwbVWO).

In meiner Antwort an die Arbeitsgemeinschaft teilte ich mit, dass ein öffentlicher Aushang dieser Liste am „Schwarzen Brett“ einer Behörde nach meiner Auffassung aus datenschutzrechtlicher Sicht unzulässig ist. Denn bei dieser Verfahrensweise würde jedem Angehörigen der Dienststelle und eventuell sogar außenstehenden Personen wie Besuchern bekannt, wer in einer Dienststelle schwerbehindert ist. Eine solche Offenbarung ihrer personenbezogenen Daten müssten die Betroffenen nur hinnehmen, wenn dies zur ordnungsgemäßen Durchführung der Wahl der Schwerbehindertenvertretung erforderlich wäre. Das ist meines Erachtens nicht der Fall.

Das Wählerverzeichnis ist zur Einsicht auszulegen, damit es von den dazu Berechtigten auf seine Richtigkeit hin überprüft werden kann. Ein Einspruchsrecht gegen die Liste der Wahlberechtigten steht nicht jedem Angehörigen der Dienststelle zu. Dieses Recht haben vielmehr nur die Wahlberechtigten und die übrigen Beschäftigten dann, wenn sie ein berechtigtes Interesse an einer ordnungsgemäßen Wahl glaubhaft machen können (§ 4 Abs.1 S.1 SchwbVWO). Da somit nicht jeder Angehörige einer Dienststelle ein Einsichtsrecht besitzt, darf die Liste nicht allgemein zugänglich gemacht werden.

13.8 Videoüberwachung eines Serverraumes

In einer größeren Behörde des Saarlandes ist eine Videoüberwachungsanlage im Serverraum installiert worden. Der Örtliche Personalrat bat mich daraufhin um meine datenschutzrechtliche Bewertung.

Die Videoüberwachung von Serverräumen größerer Behörden oder Firmen gehört mittlerweile zur standardisierten Technik, die zur Gewährleistung des Sicherheitsstandards beitragen soll. Allerdings besteht somit auch die Möglichkeit, Beschäftigte der betreffenden Behörde, die Zutritt zum Serverraum haben zu überwachen. Die zentrale Frage, mit der ich mich beschäftigen musste, lautet: „Ist das Recht auf informationelle Selbstbestimmung der Mitarbeiter höher anzusiedeln als die Sicherheitsvorkehrungen im Serverraum?“

Dazu musste ich mich zuerst kundig machen, welche Möglichkeiten die Videoüberwachungsanlage hat. Nach Rücksprache mit dem zuständigen Techniker der Behörde ergab sich Folgendes: Die Videoüberwachungsanlage besteht aus 3 Kameras. Sie zeichnen nur bei Bildveränderungen auf und senden diese Daten über das Netzwerk an einen Server. Die Kameras speichern keine Filmsequenzen, sondern lediglich Einzelbilder im zeitlichen Abstand. Sie besitzen eine eigene binäre Dateiverwaltung innerhalb der Kamera und verwalten damit alle erstellten und gespeicherten Daten selbst. Über diese Dateiverwaltung lösen die Kameras entsprechend der definierten Aufbewahrungsfrist von 4 Wochen die Löschung automatisch aus. Der Zugriff auf die gespeicherten Daten haben drei namentlich benannte Mitarbeiter, die in der Administration tätig sind. Daneben haben lediglich der Sachgebietsleiter und sein Vertreter Zugriffsrechte. Der Zugriff kann nur über 5 explizit definierte PCs erlaubt werden und nur unter Verwendung von Passwörtern, die lediglich den eben genannten Personen bekannt sind. Eine Einsichtnahme der aufgezeichneten Bilder ist nur bei besonders begründeten Vorkommnissen auf Weisung des Direktors oder eines bestimmten Abteilungsleiters vorgesehen.

Unter den oben angeführten Voraussetzungen bin ich der Meinung, dass die Maßnahmen zur Erhöhung der Sicherheit im Serverraum das Recht auf informationelle Selbstbestimmung der Mitarbeiter lediglich in einem datenschutzrechtlich vertretbaren Umfang tangieren.

13.9 Online-Testrechner Zahnersatz

Bei der Ruhegehalts- und Zusatzversorgungskasse des Saarlandes (RZVK des Saarlandes), einer Behörde, die unter anderem die Beihilfe für Beamte von Kommunen im Saarland berechnet, war die Einführung eines Online-Testrechners für Zahnersatz geplant. Mit diesem Programm sollte Beihilfeberechtigten der Mitglieder der Umlagegemeinschaft die Möglichkeit gegeben werden, die voraussichtliche Beihilfe vor einer Zahnersatzbehandlung zu ermitteln. Dabei müssen sich die Beihilfeberechtigten zunächst im Internet auf der Seite www.rzvk-saar.de mit ihrer Kennnummer (einer Art Mitgliedsnummer) und ihrem Geburtstag in den geschützten Mitgliederbereich einloggen. Im Vorfeld der Berechnung müssen sie einen Behandlungsplan von ihrem Zahnarzt ausfüllen lassen, aus dem die für die Berechnung relevanten Daten hervorgehen. Diese Daten und die persönlichen Daten der Mitglieder werden dann im Internet eingegeben und das Programm errechnet selbständig die zu erwartende Beihilfe. Gemäß § 7 Abs. 2 SDSG wurde ich vor dem erstmaligen Einsatz des automatisierten Verfahrens gehört. Durch die vorbildliche Zusammenarbeit der RZVK mit meiner Geschäftsstelle konnten datenschutzrechtliche Probleme schon im Vorfeld der Einführung beseitigt werden. So wurde unter anderem das Einloggen erst im geschützten https-Bereich des Internetangebotes erreicht und die komplette Testrechnung aufgrund meines Vorschlages lediglich ein halbes Jahr für Beihilfezwecke bei der RZVK gespeichert. All unseren Bedenken wurde Rechnung getragen und das Programm nach unseren Wünschen umgestaltet. So konnte nach Erstellung des Verfahrensverzeichnisses gemäß § 9 SDSG eine datenschutzfreundliche Serviceleistung der RZVK für Ihre Mitglieder zur Verfügung gestellt werden.

14 Rundfunk und Medien, Telekommunikation

14.1 Befreiung von der Rundfunkgebührenpflicht

Empfänger bestimmter Sozialleistungen werden von der Rundfunkgebührenpflicht befreit. Zu dem berechtigten Personenkreis zählen z.B. Empfänger von Sozialhilfe, von Arbeitslosengeld II, von Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz oder Empfänger von Leistungen nach dem Asylbewerberleistungsgesetz.

Um in den Genuss der Befreiung zu kommen, musste bisher bei der zuständigen Gemeinde ein Antrag gestellt werden, auf dem die Gemeinde das Vorliegen der Befreiungsvoraussetzungen bescheinigte. Über den Antrag entschied die Rundfunkanstalt auf Vorschlag der Gemeinde. Rechtsgrundlage dieser Verfahrensweise war die saarländische „Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht“.

Dieses Verfahren wurde durch eine Änderung des Rundfunkgebührenstaatsvertrages so geändert, dass nunmehr die Anträge auf Befreiung von der Rundfunkgebührenpflicht ausschließlich von den zuständigen Landesrundfunkanstalten entschieden werden (§ 6 Absatz 4 RGebStV).

Datenschutzrechtlich brisant ist in diesem Zusammenhang die Neuregelung des § 6 Absatz 2 RGebStV, wonach die Antragsteller verpflichtet sind, das Vorliegen der Befreiungsvoraussetzungen durch die Vorlage des jeweiligen Bescheides im Original oder in beglaubigter Kopie nachzuweisen. In diesen Bescheiden sind eine Vielzahl sensibler personenbezogener Daten enthalten (z.B. Informationen über die Einkommens-, Vermögens- und Wohnsituation der Antragsteller), die die GEZ für die Entscheidung über die Befreiung überhaupt nicht benötigt. Für die GEZ ist im Wesentlichen nur wichtig, um welche Art von Sozialleistungen es sich handelt sowie für welchen Zeitraum die Leistung bewilligt wurde.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich nach Bekanntwerden dieser Änderung und nach zahlreichen Beschwerden betroffener Bürger darum bemüht, eine Änderung des maßgeblichen § 6 Absatz 2 RGebStV zu erreichen. Nach längeren Verhandlungen mit der Rundfunkseite haben sich die Landesbeauftragten für den Datenschutz mit den Rundfunkbeauftragten für den Daten-

schutz auf eine gemeinsame Formulierung geeinigt, wonach der Nachweis für die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht außer durch Vorlage des entsprechenden Sozialleistungsbescheides auch durch Vorlage einer entsprechenden Bestätigung des Leistungsträgers geführt werden kann. Die Landesrundfunkanstalten und die GEZ haben sich bereit erklärt, im Vorgriff auf diese gesetzliche Regelung bereits entsprechende Bescheinigungen anzuerkennen. Es geht nunmehr darum, die Sozialleistungsträger für eine Mitarbeit zu gewinnen, indem sie entsprechende Bescheinigungen ausstellen, denn eine Verpflichtung zur Ausstellung einer entsprechenden Bescheinigung wird durch die geplante Änderung des Rundfunkgebührenstaatsvertrages nicht begründet.

15 Landwirtschaft

15.1 Berichtsheftführung im Ausbildungsberuf „Landwirt/in“

In einer Anfrage eines Kollegen aus einem anderen Bundesland wurde zur Diskussion gestellt, ob es zulässig ist, während der Ausbildung zum/zur Landwirt/in in dem von der Ausbildungsverordnung vorgeschriebenen Berichtsheft (§ 7 Verordnung über die Berufsausbildung zum Landwirt/Landwirtin), betriebseigene Daten der Ausbilder aufzuführen, die bei einem Betriebswechsel während der Ausbildung dem Nachfolgebetrieb offenbart werden. In dem Berichtsheft soll dem Auszubildenden betriebswirtschaftliches Grundwissen vermittelt werden. So sind zum Beispiel Berechnungen mit Saatgutpreisen und den zu erwartenden Erträgen vorgesehen. Teilt der Betrieb A jetzt in der Berechnung seine tatsächlichen Saatgutpreise mit, kann der Betrieb B, bei dem der zweite Ausbildungsabschnitt stattfindet anhand des Berichtsheftes sehen, dass Betrieb A günstigere Preise für das gleiche Saatgut beim gleichen Händler erhandelt hat. Dieser Umstand kann in Einzelfällen natürlich zu Problemen führen. Auf Anregung meiner Dienststelle bei der Landwirtschaftskammer des Saarlandes wurde folgende Regelung vereinbart:

Im Antrag auf Anerkennung als Ausbildungsstätte für die Ausbildung in den Berufen des Agrarbereichs wird eine Anmerkung zur Berichtsheftführung der Auszubildenden aufgenommen, aus der hervorgeht, dass persönliche und betriebsspezifische Angaben seitens des ausbildenden Betriebes freiwillig sind. Stattdessen kann zum Beispiel eine Musterberechnung oder ein Musterbeispiel eingesetzt werden.

Zusätzlich wurde das Problem beim nächsten Zusammentreffen saarländischer Ausbilder in den Berufen des Agrarbereiches als Tagesordnungspunkt ausführlich erörtert und nochmals auf die Freiwilligkeit der betriebsspezifischen und persönlichen Angaben im Berichtsheft hingewiesen.

16 Sonstiges

16.1 Bergbaudaten für eine Gemeinde

Eine saarländische Gemeinde, die durch die untertägigen bergbaulichen Aktivitäten der Deutschen Steinkohle AG betroffen ist, plante den Aufbau einer Datei mit bestimmten Messdaten, aus denen Rückschlüsse auf die bergbaulichen Einwirkungen möglich sind. Zweck dieser Datei sollte es sein, die Gemeindeeinwohner in bergschadensrechtlichen Auseinandersetzungen zu unterstützen bzw. um in der Lage zu sein, eigene Ansprüche durchzusetzen.
Das Ministerium für Wirtschaft und Arbeit hat mich um Stellungnahme gebeten, ob der Anlegung einer solchen Datei datenschutzrechtliche Aspekte entgegenstehen.
Datenschutzrechtliche Relevanz erhält das Vorhaben dadurch, dass personenbezogene Daten der Bergverwaltung an die Gemeinde hätten übermittelt werden müssen. Auch wenn die Daten unmittelbar nur Teilkoordinaten öffentlicher Flächen wiedergeben, lassen sie jedoch auch Rückschlüsse zu auf Veränderungen benachbart anliegender privater Grundstücksflächen.
Bei der datenschutzrechtlichen Beurteilung ist zu differenzieren:
Soweit die Gemeinde die Messdaten zur Verfolgung eigener Ansprüche beanspruchte, gibt es eine entsprechende Rechtsgrundlage im Bundesberggesetz (§ 125 Absatz 1 in Verbindung mit § 63 Absatz 4 Bundesberggesetz). Wenn die Gemeinde gegenüber der Bergverwaltung glaubhaft machen kann, von einem Bergschaden betroffen zu sein, hat sie ein Recht zur Einsichtnahme in die entsprechenden Unterlagen.

Soweit die Gemeinde ihre Bürger mit Hilfe der Messdaten in bergschadensrechtlichen Auseinandersetzungen unterstützen wollte, habe ich zunächst Zweifel geäußert, ob eine solche Hilfestellung überhaupt zu dem Aufgabenbereich einer Kommune gehört. Diese Frage konnte jedoch letztlich dahingestellt bleiben, da die Voraussetzungen für eine Übermittlung der Daten von der Bergverwaltung an die Gemeinde nach den hier maßgeblichen Bestimmungen des Saarländischen Datenschutzgesetzes nicht vorliegen.
Das Ministerium hat argumentiert, dass die Erfassung der Daten offensichtlich im Interesse betroffener Grundstückseigentümer liege. Dem habe ich widersprochen, denn es ist meiner Auffassung nach genauso gut vorstellbar, dass betroffene Grund-

stückseigentümer unter dem Gesichtspunkt, dass keine wertbeeinflussenden Erkenntnisse über ihre Immobilie preisgegeben werden, den Vorrang einräumen.
Nicht zustimmen konnte ich auch dem Vorschlag der Gemeinde, eine Veröffentlichung an die Bürgerschaft zu richten und die Bürger mit Fristsetzung aufzufordern, gegebenenfalls eine Nichteinwilligung bezüglich der Übermittlung der Daten ausdrücklich zu erklären. Zwar ist nach den Datenschutzgesetzen eine Datenverarbeitung mit Einwilligung der Betroffenen möglich. Einwilligung bedeutet aber eine ausdrückliche, das Einverständnis des Betroffenen dokumentierende Erklärung. Hieran mangelt es, wenn eine Rechtsfolge eintreten soll für den Fall, dass der Betroffene sich nicht äußert.

Ich habe deshalb die Auffassung vertreten, dass eine Übermittlung der fraglichen Messdaten von der Bergverwaltung an die Gemeinde nicht zulässig ist, da weder die Einwilligung der betroffenen Bürger vorliegt, noch eine Rechtsgrundlage existiert, die die Datenübermittlung legitimieren könnte.

Zwischenzeitlich hat die betreffende Gemeinde dargetan, dass die Daten für sie wichtig seien, um rechtzeitig drohende Schäden für das kommunale Kanalsystem zu erkennen.
Sollten die fraglichen Daten für diesen Zweck tatsächlich relevant sein, was ich mangels entsprechenden technischen Sachverstandes nicht beurteilen kann, so sehe ich eine Befugnis zur Übermittlung in der Vorschrift des § 13 Abs. 2 Buchstabe e SDSG, wonach eine Datenübermittlung zulässig ist, wenn sie zur Abwehr erheblicher Gefahren für das Gemeinwohl erforderlich ist.

16.2 Brand- und Katastrophenschutzgesetz

Zum 01.01.2007 trat das Gesetz zur Neuordnung des Brand- und Katastrophenschutzrechts im Saarland in Kraft. Es hat zum Ziel, abweichend von der bisherigen Gesetzessystematik ein einheitliches Gesetz für den Brandschutz, die Technische Hilfe und den Katastrophenschutz zu schaffen.
Ich konnte erreichen, dass die Löschfrist für die bei Einsatz- und Alarmzentralen oder der Integrierten Leitstelle im Saarland eingehende Anrufe, die auch ohne Einwilligung

des Anrufers auf Tonträgern aufgezeichnet werden dürfen, mit einer Ausnahme auf drei Monate beschränkt wurde. Lediglich im Falle einer Beweismittelsicherung dürfen die Tonträger länger aufbewahrt werden. Entgegen dem Entwurf wurde somit die Speicherung über den dritten Monat hinaus zur Abwehr von Gefahren für die öffentliche Sicherheit oder von Nachteilen für das Wohl des Bundes oder eines Landes gänzlich verhindert.
Im Entwurf war vorgesehen, dass die bei Katastrophen eingerichteten Personenauskunftsstellen personenbezogene Daten im erforderlichen Umfang verarbeiten dürfen. Um transparenter zu machen, welche Art von Daten von diesen Stellen gespeichert werden, habe ich vorgeschlagen, die Zweckbestimmung der Daten im Gesetz zu benennen. Die entsprechende Vorschrift wurde dahingehend geändert, dass die Personenauskunftsstellen Daten nur insoweit verarbeiten dürfen, wie dies für Zwecke der Auskunftserteilung über den Verbleib von Betroffenen sowie für deren Registrierung und Identifizierung erforderlich ist.

16.3 Der Elektronische Einkommensnachweis (ELENA)

Über das Verfahren ELENA (Elektronischer Einkommensnachweis) habe ich bereits in meinem 20. Tätigkeitsbericht 2003/2004 (TZ 8.4) berichtet. Damals hieß das Verfahren noch JobCard.
Mit dem Verfahren ELENA sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Diese zentrale Speicherstelle soll die Daten öffentlichen Leistungsstellen auf Abruf in elektronischer Form zur Verfügung stellen.
Es ist offensichtlich, dass dieses Verfahren angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz ist.
Verfassungsrechtlich stellt sich die Frage, ob es sich hierbei um eine nach der Rechtssprechung des Bundesverfassungsgerichts unzulässige Datenspeicherung auf Vorrat handelt, da die Daten sämtlicher Bürger gespeichert werden, obwohl der Datenbestand nur für einen Bruchteil der erfassten Fälle relevant sein wird.
Zwar soll der Verwendungszweck gesetzgeberisch auf die Erteilung der genannten Bescheinigungen festgelegt werden, es ist aber zum gegenwärtigen Zeitpunkt nicht

absehbar, für welche Verwendungszwecke dieser Datenbestand in Zukunft noch genutzt werden soll. Die Problematik wird durch eine aktuelle gesetzgeberische Begrenzung des Verwendungszwecks nicht ausgeräumt, da diese jederzeit erweitert werden kann.

Von wesentlicher Bedeutung wird sein, dass das Verfahren technisch und organisatorisch so ausgestaltet ist, dass unbefugte Zugriffe ausgeschlossen sind.

Die ursprünglich ins Auge gefasste Ende-zu-Ende-Verschlüsselung der Beschäftigtendaten mit dem Schlüssel der Betroffenen scheint nach einem speziell zu dieser Frage erstellten Gutachten des Bundesamtes für Sicherheit in der Informationstechnik unrealistisch.

Maßgebend dafür sind insbesondere die komplexen Anforderungen eines solchen Verfahrens an eine völlig heterogene Datenverarbeitungsinfrastruktur bei den Arbeitgeberinnen und Arbeitgebern und der damit verbundene hohe Integrations- und Administrierungsaufwand bei den einzelnen Unternehmen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einem Beschluss auf ihrer Konferenz am 27./28.10.2005 deutlich gemacht, dass sie in einer Ver- und Entschlüsselung der Daten durch eine unabhängige Vertrauensstelle eine wichtige zusätzliche datenschutzrechtliche Sicherung im Sinn einer Teilung der Verantwortlichkeiten – Funktionelles Vier-Augen-Prinzip – sehen. Sie haben vorgeschlagen, das Konzept in diesem Sinne fortzuschreiben.

In dem gleichen Beschluss haben sie dargestellt, dass die Transparenz der Datenspeicherung und –übermittlung verbessert werden könnte, etwa dergestalt, dass für die Betroffenen eine jederzeitige elektronische Abrufmöglichkeit der gespeicherten Daten und sämtlicher Übermittlungsvorgänge, z.B. auf Basis einer Protokollierung, geschaffen wird.

16.4 Landesamt für Zentrale Dienste

Mit dem Gesetz zur Errichtung des Landesamtes für Zentrale Dienste vom 19.9.2006 wurden das Landesamt für Finanzen, das Statistische Landesamt und das Landesamt für Bau und Liegenschaften zusammengeführt. Damit wurde innerhalb der Landesverwaltung einem Vorschlag des „Hesse-Gutachtens“ Rechnung getragen.

Schon frühzeitig, ab Juni 2005, wurde der Landesbeauftragte für den Datenschutz und die Informationsfreiheit durch das federführende Ministerium der Finanzen in die Planungen eingebunden. Mein Augenmerk lag insbesondere auf der datenschutzverträglichen Eingliederung des Statistischen Landesamtes und einer entsprechenden Anpassung des Saarländischen Landesstatistikgesetzes.

Das Statistische Amt wird nunmehr als eigenständige Organisationseinheit im Landesamt für Zentrale Dienste (LZD) geführt. Es ist organisatorisch und räumlich von anderen Verwaltungsstellen des LZD und der sonstigen Landesverwaltung abgegrenzt.

Das Weisungsrecht gegenüber dem Statistischen Amt erstreckt sich nicht auf die Weitergabe von Einzelangaben, die der statistischen Geheimhaltung unterliegen. Das Personal darf während seiner Tätigkeit im Statistischen Amt nicht mit anderen Aufgaben des Verwaltungsvollzugs betraut werden.

Mit diesen Regelungen wurde den Grundsätzen Folge geleistet, die durch das Bundesverfassungsgericht in seinem Urteil zur Volkszählung aufgestellt wurden.

16.5 Swift

Bei Auslandsüberweisungen bedient sich die Kapital- und Finanzwirtschaft der Dienste einer internationalen Genossenschaft der Finanzwirtschaft namens SWIFT (Society for Worldwide Interbank Financial Telecommunications) mit Sitz in Belgien. Die Banken leiten bestimmte Daten wie Namen des Auftraggebers und des Empfängers, Betrag und Verwendungszweck an SWIFT weiter. Diese Daten werden zu Zwecke der Datensicherung auf Rechnern in Belgien und in den USA gespeichert.

Nach den Terrorangriffen am 11.9.2001 haben sich amerikanische Sicherheitsbehörden durch Beschlagnahmeanordnungen Zugriff auf die in den USA gespeicherten Daten verschafft. Dieses Vorgehen war selbst in der Finanzwelt weitgehend unbekannt und wurde erst durch die Berichterstattung der Presse veröffentlicht.

Der „Düsseldorfer Kreis“, bundesweites Gremium der obersten Aufsichtsbehörden für Datenschutz im nicht öffentlichen Bereich stellte fest, dass die praktizierte Übermittlung von Datensätzen an das SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe der gespeicherten Daten an US-amerikanische Behörden sowohl nach deutschem Recht als auch nach europäischem Datenschutzrecht unzulässig sind.

Die Banken wurden aufgefordert unverzüglich Maßnahmen vorzuschlagen, durch die im Swift-Verfahren entweder eine Datenübermittlung in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist.

Weiterhin wurden die Banken darauf hingewiesen, dass sie ihre Kundinnen und Kunden gemäß § 4 Abs. 3 Bundesdatenschutzgesetz über die Weiterleitung von Datensätzen an das SWIFT-Rechenzentrum in den USA informieren müssen.

16.6 Auskunft aus dem Bundeszentralregister an die Industrie- und Handelskammer

Aus Anlass einer Eingabe habe ich das Verfahren der Bestellung von Sachverständigen durch die Industrie- und Handelskammer des Saarlandes (IHK Saarland) überprüft.

In diesem Verfahren wird auf Veranlassung der IHK Saarland durch das saarländische Wirtschaftsministerium als oberste Landesbehörde eine unbeschränkte Auskunft aus dem Bundeszentralregister eingeholt. Die unbeschränkte Auskunft wurde zur Bewertung der persönlichen Eignung herangezogen.

Diese Praxis steht nicht im Einklang mit den §§ 41, 43 Bundeszentralregistergesetz (BZRG):

- § 41 BZRG enthält eine abschließende Aufzählung, wem die unbeschränkte Auskunft erteilt werden darf. Die Industrie- und Handelskammern sind nicht aufgeführt.
- § 43 BZRG regelt die Weitergabe durch die obersten Landesbehörden. Eine Weitergabe ist nur zulässig, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde.

Im Antragsverfahren selbst wurde von den Bewerbern zur Beurteilung der persönlichen Eignung lediglich eine Selbstauskunft darüber abverlangt, dass sie in geordneten wirtschaftlichen Verhältnissen leben sowie die Nennung von 4 – 5 Personen, die Auskunft über den Bewerber geben können. Ein Hinweis, dass die unbeschränkte Auskunft eingeholt wird, fehlte und wurde erst nach meiner Prüfung in ein Hinweisblatt übernommen.

Im Vergleich mit anderen Bundesländern konnte ich feststellen, dass dort die Vorlage eines polizeilichen Führungszeugnisses als ausreichend erachtet wird.

Unter Darlegung dieser Aspekte konnte ich in Abstimmung mit dem saarländischen Wirtschaftsministerium erreichen, dass in Zukunft auf die Einholung einer unbeschränkten Auskunft verzichtet wird. Auch im Saarland genügt zukünftig die Vorlage des Führungszeugnisses.

17 Anlagen

17.1 Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse

Die strafprozessuale DNA-Analyse ist - insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten - ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z.B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber - auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung - in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche

Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

17.2 Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005 in Kiel

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und –interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und –interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

17.3 Erhebung und Übermittlung personenbezogener Daten im Akkreditierungsverfahren zur Fußball-Weltmeisterschaft 2006

Beschluss eines gemeinsamen Schreibens an den Deutschen Fußballbund, die Projektgruppe UAFEK WM 2006 bei der Bezirksregierung Köln und die Innenministerien des Bundes und der Länder

Schreiben des Regierungspräsidiums Darmstadt vom 17. Februar 2005

Sehr geehrte Damen und Herren,
im Rahmen der Fußball-Weltmeisterschaft 2006 will der Deutsche Fußballbund (DFB) in Zusammenarbeit mit den Polizeibehörden ca. 160.000 - 170.000 Personen einer “Zuverlässigkeitsüberprüfung" unterziehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet die undifferenzierte und massenhafte Erfassung von Beteiligten an Sportveranstaltungen anlässlich der Fußball-Weltmeisterschaft 2006 mit großer Sorge. Personen, die aus unterschiedlichen Gründen in den Stadien tätig sein sollen, sind danach einem Akkreditierungsverfahren zu unterwerfen, um für die Stadien eine Zugangsberechtigung zu erhalten. Hierfür sollen Arbeitgeber Daten ihrer eingesetzten Mitarbeiterinnen bzw. Mitarbeiter an den DFB übermitteln. Auch freiberuflich tätige Bewerberinnen und Bewerber müssen ihre Daten dem DFB zur Verfügung stellen. Der DFB will die Daten an die Landeskriminalämter und an das Bundeskriminalamt weiterleiten. Diese Polizeibehörden sollen die Daten mit ihren polizeilichen Dateien abgleichen und dem DFB mitteilen, ob im Einzelfall “Bedenken" gegen die Akkreditierung bestehen oder nicht. Grundlage des Verfahrens soll die Einwilligung der betroffenen Personen sein.
Das Akkreditierungsverfahren weist aus datenschutzrechtlicher Sicht offene Fragen auf. So ist z.B. noch nicht im Einzelnen geklärt, wer verantwortliche Stelle für die jeweiligen Schritte der Datenverarbeitung sein soll und ob der Kreis der zu überprüfenden Personen nicht enger gefasst werden kann. Zudem ist das geplante Akkreditierungsverfahren nicht in allen Bundesländern allein aufgrund einer Einwilligung der Betroffenen zulässig; es bedarf in diesem Fall ergänzend einer besonderen gesetzlichen Grundlage. Gleichwohl weise ich (als Vorsitzender der Konferenz der

Datenschutzbeauftragten des Bundes und der Länder) in Absprache mit meinen Kolleginnen und Kollegen aus den anderen Bundesländern und dem Bundesbeauftragten für Datenschutz bereits jetzt auf einige wichtige datenschutzrechtliche Aspekte hin, die zu beachten sind:

Die Daten dürfen nur erhoben und weiterverarbeitet werden, wenn und soweit dies für die Durchführung des Akkreditierungsverfahrens zwingend erforderlich ist.

Die betroffenen Personen sind über den Ablauf des Akkreditierungsverfahrens umfassend zu informieren. Sie sind aufzuklären, welche personenbezogenen Daten erfasst und an welche Stellen diese Daten übermittelt werden. Es muss den Betroffenen erkennbar sein, mit welchen polizeilichen Datensammlungen diese abgeglichen werden. Sie sind darauf hinzuweisen, dass in begründeten Einzelfällen auch eine Überprüfung (in zu bezeichnenden Dateien) des Verfassungsschutzes erfolgt.

Die Betroffenen müssen sich eine Vorstellung darüber machen können, welche von ihnen ggf. begangenen Aktivitäten wie z.B. Straftaten ihrer Zuverlässigkeit entgegenstehen können und ob dies auch für eingestellte Verfahren gilt.

Die Transparenz des Verfahrens ist gefährdet, wenn die Betroffenen die Antragsformulare nicht selbst ausfüllen, sondern ihre Arbeitgeber dies für sie “erledigen". Dadurch wäre für die Betroffenen nicht ohne weiteres erkennbar, welche personenbezogenen Daten die Arbeitgeber an den DFB und dieser an die Polizeibehörden und etwaige weitere Stellen weitergeben. Den Betroffenen ist also neben der Datenschutzerklärung auch das Antragsformular für die Akkreditierung mit den persönlichen Angaben auszuhändigen. Ohne eine wirksame Einwilligung der Betroffenen ist eine Übermittlung ihrer Daten durch den Arbeitgeber an den DFB in der Regel nicht zulässig.

Die Datenabgleiche dürfen nur durchgeführt werden, wenn und soweit dies nach dem jeweiligen Polizeirecht im Hinblick auf den Zweck der jeweiligen Datei im Einzelfall zulässig ist.

Die bisherigen Unterlagen sehen vor, dass der Arbeitgeber vom DFB über das Ergebnis der “Zuverlässigkeitsüberprüfung" informiert wird und dieser dann die Arbeitnehmerin oder den Arbeitnehmer informiert.

Bei einer Übermittlung direkt an den DFB und von diesem an den Arbeitgeber ist es problematisch, dass die betroffene Person zuvor nicht gehört würde, bevor die Daten an die dritte Stelle übermittelt werden. Die Polizeigesetze enthalten unter-

schiedliche Regelungen, unter welchen Umständen die Polizeibehörden befugt sind, ihre Daten an private Stellen zu übermitteln.

Das Ergebnis der Überprüfung sollte deshalb direkt der betroffenen Person selbst in Form einer Unbedenklichkeitsbestätigung ausgehändigt werden. Diese kann die Bescheinigung sodann dem DFB und ihrem Arbeitgeber vorlegen. Dieses Verfahren ist weniger eingriffsintensiv als das bislang vorgesehene Verfahren. Den Betroffenen steht es dann frei, die Bewerbung zurückzuziehen, bevor Dritte über etwaige “Sicherheitsbedenken" informiert werden. Dies betrifft nicht nur freiberuflich tätige Bewerberinnen und Bewerber, sondern auch Arbeitnehmerinnen und Arbeitnehmer, die sich innerbetrieblich für eine Mitwirkung an der Fußball-WM beworben haben. Zudem erhalten die Betroffenen die Möglichkeit, etwaige Unregelmäßigkeiten (unzulässige oder falsche Auskünfte, falsche Zuordnungen) direkt mit den Sicherheitsbehörden zu klären und sich zu den Umständen zu äußern, auf denen die Bedenken beruhen. Im Falle eines Irrtums oder einer unzulässigen Datenspeicherung (z.B. einer versäumten Aussonderungsprüffrist) ist so eine Korrektur möglich, bevor der DFB und der Arbeitgeber von der Speicherung erfahren.

Ich bitte Sie, bei der weiteren Gestaltung des Verfahrens die vorstehenden Überlegungen auch bei der Ausgestaltung der Datenschutzerklärung des Regierungspräsidiums Darmstadt (Stand: 16.02.2005) zu berücksichtigen und mitzuteilen, welches Verfahren letztendlich gewählt wird.

Mit freundlichen Grüßen

17.4 Einführung der elektronischen Gesundheitskarte

Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005 in Kiel

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen - technischen wie organisatorischen - Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

17.5 Brief an die Bundesministerin der Justiz

69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005 in Kiel

Inhaltliche Festlegung für einen Brief an die Bundesministerin der Justiz

Die Konferenz der Datenschutzbeauftragten weist zu den Überlegungen für eine Regelung von DNA-Massen-Screeningmaßnahmen auf Folgendes hin:

- Die DNA-Analyse zur Identitätsfeststellung stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Von ihr sind regelmäßig ganz überwiegend Unverdächtige betroffen.
- Deshalb darf von diesem Instrument nur bei Verbrechen gegen das Leben, die körperliche Unversehrtheit, die Freiheit oder die sexuelle Selbstbestimmung und nur dann Gebrauch gemacht werden, wenn andere Möglichkeiten zur Aufklärung der Tat nicht mehr bestehen.
- Der Umfang des Massen-Screenings muss auf der Grundlage einer nachvollziehbaren Tat- oder Täterhypothese und so differenziert bestimmt werden, dass die Zahl der einbezogenen Personen möglichst gering gehalten werden kann.
- Das DNA-Massen-Screening darf nur auf der Grundlage einer richterlichen Entscheidung erfolgen.
- Die DNA-Analyse einer nicht beschuldigten Person darf nur mit deren Einwilligung durchgeführt werden.
- Eine Nichterteilung der Einwilligung darf allein einen Tatverdacht nicht begründen.
- Für eine wirksame Einwilligung ist eine rechtzeitige und umfassende Information über Erhebungszweck, Freiwilligkeit, Nutzung und Löschung des Probenmaterials und der daraus gewonnenen Untersuchungsergebnisse erforderlich.
- Die Auswertung der Proben ist entsprechend § 81 f StPO durchzuführen.
- Die Proben sind unverzüglich nach der Erstellung der DNA-Identifizierungsmuster zu vernichten. Die Muster dürfen nur mit den Tatortspuren abgeglichen werden. Eine Zweckänderung ist unzulässig.
- In Nichttrefferfällen sind die Identifizierungsmuster unverzüglich zu löschen

17.6 Einführung biometrischer Ausweisdokumente

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Juni 2005

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,

- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

17.7 Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisheri-

gen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

17.8 Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

17.9 Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechtes. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öf-

fentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der Ausforschung ihrer Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen Evaluierung durch unabhängige Stellen unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der Leistungs- und Finanzkontrolle die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen

die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.
Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte Arbeitnehmerdatenschutzgesetz muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher Datenschutz in der Europäischen Union gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

17.10 Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung –und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Ge-

währleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.
Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u.a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

17.11 Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

17.12 Telefonieren mit Internettechnologie (Voice over IP - VoIP)

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internet-Telefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter

im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,

Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,

Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,

auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,

VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und

bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

17.13 Keine Vorratsdatenspeicherung in der Telekommunikation

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005 in der Hansestadt Lübeck

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und –partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzel-

nen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z.B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.
Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsda-

tenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

17.14 Sicherheit bei eGovernment durch Nutzung des Standards OSCI

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

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.
Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partner.
Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.
Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.
Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den

Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

17.15 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. - 17. März 2006 in Magdeburg

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

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

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

17.16 Keine kontrollfreien Räume bei der Leistung von ALG II

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. - 17. März 2006 in Magdeburg

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

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

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

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

17.17 Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. - 17. März 2006 in Magdeburg

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

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

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

Dies bedeutet u.a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit

der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt - einbeziehen.

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

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

17.18 Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. - 17. März 2006 in Magdeburg

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

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

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

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis un-

terliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

17.19 Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

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

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

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

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen

Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.
- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.
- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.
- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.
- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

17.20 Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

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

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

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

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

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

17.21 Verbindliche Regelungen für den Einsatz von RFID-Technologien

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

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

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

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

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informations-

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

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

Transparenz:

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

Kennzeichnungspflicht:

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

Keine heimliche Profilierung:

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

- *Vermeidung der unbefugten Kenntnisnahme:*

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

- *Deaktivierung:*

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

17.22 Keine Schülerstatistik ohne Datenschutz

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

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

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

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

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

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

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

17.23 Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Entschließung vom 11. Oktober 2006 (bei Enthaltung von Schleswig-Holstein)

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

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

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

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikati-

onspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

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

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

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

Dies bedeutet, dass

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

- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.
Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

17.24 Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten

27. Internationale Konferenz der Datenschutzbeauftragten Montreux, 16. September 2005

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschliesst:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zur Zeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschliessen, um zum einen den Terrorismus bekämpfen und zum andern Grenzkontrollen und Check-in-Verfahren beschleunigen zu können;

Wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis;

Unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann;

Im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar" machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten;

Unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte;

fordert die Konferenz

wirksame Schutzmassnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und

gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,
die technische Beschränkung der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage.

18 Sachverzeichnis

19 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
BSI	Bundesamt für Sicherheit in der Informationstechnik
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
KSVG	Kommunalselbstverwaltungsgesetz
LfD	Landesbeauftragter für Datenschutz

LSVS	Landessportverband Saar
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
MBKW	Ministerium für Kultur, Bildung und Wirtschaft
MeldDÜV	Meldedatenübermittlungsverordnung
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
SVerfSchG	Saarländisches Verfassungsschutzgesetz
StVollzG	Strafvollzugsgesetz
TB	Tätigkeitsbericht
TCPA	Trusted Computing Platform Alliance
Tbg-Nr.	Tagebuchnummer
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TZ	Textziffer
UIG	Umweltinformationsgesetz
USB	Universal serial bus
VG	Verwaltungsgericht